VOIP:N TIETOTURVA JA SOVELTUVUUS JULKISHALLINTOON

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2007
Juha Viitala

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

VIITALA, JUHA: VoIP:n tietoturva ja soveltuvuus julkishallintoon

Tietoliikennetekniikan opinnäytetyö, 77 sivua, 15 liitesivua

Kevät 2007

TIIVISTELMÄ

VoIP eli internet-puhelut on nykyaikainen puhelintekniikka. VoIP:n avulla voidaan siirtää ääntä ja videokuvaa reaaliaikaisesti internetin välityksellä. VoIP perustuu yleiseen ja hyväksi todettuun IP-tekniikkaan, jossa tieto kulkee verkossa IP-paketteina. VoIP on yleistymässä nopeasti niin yrityksissä, julkishallinnossa kuin kuluttajienkin keskuudessa. VoIP-tekniikan etuina ovat sen edullisuus ja joustavuus.

VoIP:n käytön yleistymisen myötä sen tietoturva on noussut puheenaiheeksi. Koska internet on koko maailman laajuinen avoin verkko, uhkat tulevat joka suunnasta. VoIP on yhtä avoin internetin uhkille, kuin muukin internetiä käyttävä tekniikka. Niinpä VoIP tarvitsee tietoturvaa, jotta uhkat voidaan estää. VoIP:ssa itsessään ei ole tietoturvaa, mutta VoIP:n kanssa voidaan käyttää olemassa olevia tietoturvaratkaisuja.

Tämä opinnäytetyö käsittelee VoIP-tekniikkaa ja sen tietoturvaa Suomen valtiohallinnon tietoturvallisuusnäkökulmasta. Valtiohallinto on ottanut tietoturvaohjeistuksessaan huomioon myös VoIP-tekniikan ja sen heikon tietoturvan. Tässä työssä tutkitaan erilaisia VoIP-järjestelmään kohdistuvia uhkia. Samoin tutkitaan ratkaisuja uhkien torjumiseksi sekä tietoturvan parantamiseksi. Merkittävimmät tietoturvaratkaisut ovat VoIP:n sijoittaminen omaan VLAN:iin sekä puheliikenteen salaus. VoIP-järjestelmä tulee myös suunnitella niin kuin mikä tahansa kriittinen palvelu.

Tietoturva huomioon ottaen ja nykyaikaisia tunnettuja turvamenetelmiä käyttäen VoIP:sta on mahdollista saada tietoturvallinen ratkaisu organisaation tai yrityksen puhelinjärjestelmäksi. Tulevaisuudessa VoIP tulee yleistymään sen kustannustehokkuuden myötä. Huolellisella suunnittelulla VoIP:sta saadaan hyvä ja toimiva puhelinratkaisu, mutta tietoturvaan tulee kuitenkin kiinnittää erityistä huomiota.

Asiasanat: VoIP, SIP, tietoturva, julkishallinto

Lahti University of Applied Sciences
Faculty of Technology

VIITALA, JUHA: Data security of VoIP and its suitability for public administration

Bachelor's Thesis in Telecommunications Technology, 77 pages, 15 appendices

Spring 2007

ABSTRACT

VoIP or internet calls is a modern phoning technology. With VoIP it is possible to transfer voice and video in real-time through internet. VoIP is based on common and well established IP technology, where the information travels over the network in the form of IP packets. VoIP is fast becoming more general in companies, in government and among consumers. The benefits of the VoIP technology are low cost and flexibility.

Since the use of VoIP has became more general, its security has also became a topic. Because the internet is a world-wide, open network, there are threats coming from everywhere. VoIP is as open to the threats on internet as other technologies using internet. So VoIP needs data security to prevent the threats. In VoIP itself does not have any data security, but existing data security solutions can be used with VoIP.

This thesis handles VoIP technology and its data security from the point of the data security of the Finnish government. The government has taken VoIP technology and its weak security into account in its instructions concerning data security. In this thesis, different threats which are directed to VoIP systems, are examined. Also solutions to resist the threats and to improve data security are discussed. The most significant data security solutions are to assign VoIP to its own VLAN and securing the call traffic. A VoIP system should be designed as any other critical service.

When data security has been considered and modern security methods have been used, it is possible to make VoIP a secure phoning solution for the organizations or companies. In the future VoIP will become more general because of its cost-effectiveness. With careful planning it is possible to make VoIP a good and working phoning solution, but special attention should be paid to the data security.

Keywords: VoIP, SIP, data security, public administration

SISÄLTÖ

1 JOHDANTO 1
1.1 VoIP 1
1.2 Opinnäytetyön rajaus ja tavoitteet 1

2 VOIP:N PERUSTEET 2
2.1 IP-pohjainen tekniikka 2
2.2 Internet-verkko 2
2.3 Internet-protokolla 4

3 VOIP:N TEKNIIKAT JA STANDARDIT 5
3.1 Merkinanto 5
3.1.1 Perinteisen puhelinverkon merkinanto 5
3.1.2 H.323-protokolla 6
3.1.3 SIP-protokolla 7
3.1.4 SIP-järjestelmän komponentit 8
3.1.5 SIP:n ominaisuudet ja toiminta 9
3.1.6 SIP vs. H.323 12
3.2 Puheen siirto 12
3.2.1 Palvelun laatu, QoS 12
3.2.2 Puheen koodaus 13
3.2.3 Reititys 15
3.3 Yhdysliikenne 15
3.3.1 Yhdysliikenne VoIP-järjestelmien välillä 15
3.3.2 Yhdysliikenne yleiseen puhelinverkkoon 16
3.3.3 ENUM – Elektroninen numerointi 16
3.4 VoIP:n edut 17
3.5 EU-lainsäädäntö 18

4 VOIP:N TIETOTURVA 19
4.1 Tietoturva 19
4.2 VoIP:n kohdistuvat uhkat 20
4.3 SIP-protokollan tietoturvauhkat 22
4.4 VoIP:n järjestelmätietoturvallisuus 25
4.4.1 VoIP-järjestelmän turvaaminen 25

4.4.2 VoIP-palvelimen turvaaminen 26
4.4.3 Haavoittuvuuksien hallinta 26
4.5 VoIP:n fyysinen tietoturva 27
4.5.1 Fyysisen ympäristön turvaaminen 27
4.5.2 VoIP- ja dataverkon erottelu 28
4.5.3 IP-osoitteiden erottelu 28
4.5.4 VoIP-VLAN 29
4.5.5 Pääsynhallinta 31
4.5.6 VLAN:ien välinen turvallisuus 32
4.6 SIP-protokollan turvaaminen 33
4.6.1 SIP:n tietoturvavaatimukset 33
4.6.2 SIP-istunnon turvaaminen 35
4.6.3 Kuljetus- ja verkkotason tietoturvamekanismit 36
4.7 RTP-protokollan turvaaminen 40
4.8 VoIP, palomuuri ja NAT 41
4.8.1 Palomuuri- ja NAT-ongelmat 41
4.8.2 Ratkaisuja VoIP:n palomuuri- ja NAT-ongelmiin 43
4.9 Käyttäjän todennus VoIP:ssa 44

5 TIETOTURVA JULKISHALLINNOSSA 46
5.1 Valtion tietoturvallisuus 46
5.1.1 Julkishallinnon rakenne 46
5.1.2 Valtiovarainministeriö vastaa valtion tietoturvallisuudesta 46
5.1.3 Valtion tietoturvallisuuden lähtökohdat 48
5.2 Valtiohallinnon keskeiset tietojärjestelmät 49
5.3 Valtiohallinnon tietoliikenneturvallisuusohjeistus 50
5.3.1 Tietoliikenneturvallisuus 50
5.3.2 Palomuurit ja verkon varmistukset 51
5.3.3 Verkon operointi ja valvonta 52
5.3.4 Langattomat tietoliikenneyhteydet 52
5.3.5 Ulkopuoliset yhteydet 53
5.3.6 Verkon eheys, käytettävyys ja luottamuksellisuus 53
5.4 Valtiohallinnon ohjeet IP-puhelinliikennettä varten 54
5.5 Valtiohallinnon laitteistoturvallisuusohjeistus 55
5.6 Valtiohallinnnon ohjeet tunnistautumiseen 55

5.6.1 Yleiset linjaukset 55
5.6.2 Verkkopalveluiden luokittelu 56
5.6.3 Käyttäjän tunnistamisen luotettavuus 57
5.6.4 Käyttäjän todentamisen luotettavuus 58
5.6.5 PKI-infrastruktuuri 59
5.7 Viestintäviraston määräykset operaattoreille 61
5.7.1 Viestintävirasto valvoo teleyritysten tietoturvallisuutta 61
5.7.2 Sähköposti- ja internet-yhteyspalvelujen tietoturvamääräykset 62
5.7.3 Tietoturvaloukkauksista ilmoittaminen 63

6 RATKAISUT VOIP:N KÄYTTÄMISEKSI JULKISHALLINNOSSA 64
6.1 Yleistä 64
6.2 VoIP:n tietoturvaratkaisut 65
6.2.1 VAHTIn aineisto ratkaisujen pohjana 65
6.2.2 Fyysisen ympäristön turvaratkaisut 65
6.2.3 VoIP-verkon turvaratkaisut 66
6.2.4 Tunnistamis- ja autentikointiratkaisut 67

7 YHTEENVETO JA JOHTOPÄÄTÖKSET 69
7.1 VoIP:n soveltuvuus julkishallinnon käyttöön 69
7.2 Työn onnistuminen 69
7.3 Tulevaisuus 71

LÄHTEET 72

LIITTEET 78

TYÖSSÄ KÄYTETYT LYHENTEET

2.5G, 3G	Lyhenne, jota käytetään eri sukupolvien matkapuhelinteknologioista
3DES	Triple Data Encryption Standard, salausalgoritmi
802.1X	Lähiverkoissa käytettävä porttikohtainen autentikointistandardi
AES	Advanced Encryption Standard, vahva salausmenetelmä
ALG	Application Level Gateway, sovellustason yhdyskäytävä
ARPA	Advanced Research Projects Agency, USA:n puolustusministeriön tutkimushanke
ATM	Asynchronous Transfer Mode, nopea yhteydellinen paketinvälitystekniikka
DHCP	Dynamic Host Configuration Protocol, protokolla IP-osoitteiden jakamiseksi verkon laitteille
DDoS	Distributed Denial of Service, palvelunestohyökkäys
DNS	Domain Name System, internetin nimipalvelujärjestelmä
DTMF	Dual-tone Multi-Frequency, äänitaajuusvalintatapa
E.164	Standardi kansainvälisille puhelinnumeroille
EDGE	Enhanced Data rates for Global Evolution, 3G-matkapuhelinteknologia
ENUM	Telephone Number Mapping, perinteisen puhelinnumeron internet-verkkotunnus
ESP	Encapsulation Security Payload, IPSec-protokollan turvalaajennus
FCP	Firewall Control Proxy, palomuuria ohjaava välityspalvelin
G.729, G.726, G.711, G.723.1	koodekkeja äänen koodaamiseen
GPRS	General Packet Radio Services, GSM-verkon pakettikytkentäinen tiedonsiirtopalvelu
GSM	Global System for Mobile Communications, matkapuhelinstandardi
H.323	VoIP:n merkinantoprotokolla
HSDPA	High-Speed Downlink Packet Access, matkapuhelinviestinnän tiedonsiirtoprotokolla
HTTP	Hypertext Transfer Protocol, kommunikointiprotokolla, joka mahdollistaa nettiselailun
HTTPS	HTTP over Secure Sockets Layer, HTTP-yhteyden salausprotokolla

IETF	Internet Engineering Tasking Force, internetin protokollista vastaava organisaatio
IKE	Internet Key Exhange, avaintenvaihtoprotokolla
iLBC	Puheen koodaamiseen tarkoitettu lisenssivapaa koodekki
IP	Internet Protocol (IPv4, IPv6), internetin tiedonsiirtoprotokolla
IPSec	Internet Protocol Security Architecture, internet-yhteyksien turvaamiseen tarkoitettu protokollaperhe
ISDN	Integrated Services Digital Network, piirikytkentäinen puhelinverkkojärjestelmä
ITU-T	International Telecommunication Union Telecommunication Standardization Sector, kansainvälinen televiestintäliitto
LAN	Local Area Network, lähiverkko
MAC	Media Access Control, ethernetin käyttämä fyysinen laiteosoite
MD5	Salausalgoritmi
MCU	Multipoint Control Unit, videoneuvottelusilta
MEGACO	Media Gateway Control Protocol, protokolla, joka mahdollistaa IP-verkon ja puhelinverkon välisten mediayhdyskäytävien ohjaamisen
MIME	Multipurpose Internet Mail Extensions, standardi, joka määrittelee tavan välittää sähköpostia
NAT	Network Address Translation, osoitteenmuunnostekniikka
OSI	Open Systems Interconnection, tietoliikennejärjestelmien suunnittelustandardi
PBX	Private Branch Exchange, perinteinen puhelinvaihdejärjestelmä
PCM	Pulse Code Modulation, pulssikoodimodulaatio
PGP	Pretty Good Privacy, järjestelmä tietojen salaukseen
PKI	Public Key Infrastructure, julkisen avaimen järjestelmä
PSK	Phase Shift Keying, modulaatiomenetelmä tai Pre-Shared Key, salausmenetelmä
PSTN	Public Switched Telephone Network, analoginen puhelinverkko
QoS	Quality of Service, tietoliikenteen palvelun laatua kuvaava termi
RTCP	Real-Time Transport Control Protocol, protokolla, joka raportoi RTP-protokollan palvelunlaadusta

RTP	Real-Time Transport Protocol, UDP:n päällä toimiva protokolla reaaliaikaisen äänen kuljetukseen
SBC	Session Border Controller, laite, jonka kautta operaattorin yhdysliikenne maailmaan kulkee
SDH	Synchronous Digital Hierarchy, synkronoidun tiedonsiirron standardi
SDP	Session Description Protocol, multimediayhteyksien kuvaamiseen tarkoitettu protokolla
SHA-1	Secure Hash Algorithm, salausalgoritmi
SIP	Session Initiation Protocol, IP-puheluiden merkinantoprotokolla
SIPS URI	SIP Secure Universal Resource Identifier, SIP-protokollan osoitemuoto, jolla voidaan määrätä suojattu yhteys
S/MIME	Secure Multipurpose Internet Mail Extensions, protokolla sähköpostin salaukseen
SMTP	Simple Mail Transfer Protocol, sähköpostiprotokolla
SPIT	Spam Over Internet Telephony, roskapostipuhelut
SSL	Secure Sockets Layer, nykyään tunnetaan nimellä TLS
STUN	Simple Traversal of UDP through NAT, palvelin, jonka avulla NAT-asiakkaat voivat saada yhteyden ulkopuoliseen VoIP-palvelimeen
TCP	Transmission Control Protocol, yhteydellinen tiedonsiirtoprotokolla
TLS	Transport Layer Security, tiedonsiirron salausprotokolla
TTP	Trusted Third Party, luotettava kolmas osapuoli
TUPAS	Suomalaisten pankkien yhteinen tunnistamispalvelu
UDP	User Datagram Protocol, yhteydetön viestinvälitysprotokolla
UMTS	Universal Mobile Telecommunications System, 3. sukupolven (3G) matkapuhelinteknologia
UPS	Uninterruptible Power System, keskeytymättömän sähkönsyötön järjestelmä
URI	Uniform Resource Identifier, merkkijono, jolla kerrotaan tiedon paikka tai nimi
URL	Uniform Resource Locator, merkkijono, jota käytetään osoittamaan WWW-sivuja
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä
VLAN	Virtual Local Area Network, virtuaalinen lähiverkko

VM	Valtiovarainministeriö
VMPS	VLAN Management Policy Server, menetelmä käyttäjän liittämiseksi oikeaan VLAN:iin
VoIP	Voice Over Internet Protocol, tekniikka, jossa ääntä ja kuvaa siirretään reaaliaikaisesti internetin välityksellä
WAN	Wide Area Network, maanlaajuinen verkko
WiMAX	Worldwide Interoperability for Microwave Access, langaton laajakaistatekniikka
WLAN	Wireless Local Area Network, langaton lähiverkko
VPN	Virtual Private Network, virtuaalinen sisäverkko
WWW	World Wide Web, hypertekstisivuista koostuva internetpalvelu
X.509	Stardardi, joka määrittelee tiedostomuodon varmenteille
xDSL	x Digital Subscriber Line, yleisnimitys digitaalisille laajakaistatekniikoille

1 JOHDANTO

1.1 VoIP

VoIP eli IP-puhe tarkoittaa puheen välittämistä IP-protokollan avulla IP-verkossa (internet, intranet ja ekstranet). VoIP:n avulla voidaan siirtää ääntä ja videota pakettimuotoisesti IP-verkossa. VoIP:ssa analoginen puhe ja videokuva muunnetaan digitaaliseen muotoon ja siirretään reaaliaikaisesti paketeissa verkon yli. Tavalliset lanka- tai matkapuhelinverkkoon soitettavat IP-puhelut kulkevat erillisen yhdyskäytävän kautta.

VoIP on levinnyt nopeasti yrityksiin, julkishallintoon, ja se on leviämässä vähitellen myös tavallisten kuluttajien keskuuteen. Lähes kaikki suuret organisaatiot ovat vähitellen siirtymässä perinteisestä lankapuhelintekniikasta VoIP-tekniikkaan sen monien etujen vuoksi. Lakeja säätelevät elimet selvittävät parhaillaan, miten VoIP tulisi ottaa huomioon lainsäädännössä.

1.2 Opinnäytetyön rajaus ja tavoitteet

Tämä opinnäytetyö käsittelee VoIP:aa julkishallinnon tietoturvallisuusnäkökulmasta. Aiheen VoIP käsittely on rajattu VoIP:n tietoturvallisuuteen. Työn tavoitteena on selvittää VoIP:n kohdistuvia tietoturvallisuusuhkia ja mahdollisia ratkaisuja uhkien välttämiseksi. Työssä pyritään tuomaan esille myös SIP-protokollaan kohdistuvia uhkia ja se, miten SIP-protokollaa voidaan turvata.

Työssä tarkastellaan myös valtionhallinnon yleisiä tietoturvavaatimuksia, -suosituksia ja -tavoitteita. Työn tavoitteena on verrata olemassa olevia VoIP:n turvaratkaisuja valtiohallinnon tietoturvavaatimuksiin. Niiden pohjalta pyritään selvittämään tietoturvaratkaisut, jotka täyttävät valtiohallinnon tietoturvavaatimukset. Lopuksi pohditaan VoIP:n soveltuvuutta julkishallinnon käyttöön.

2 VOIP:N PERUSTEET

2.1 IP-pohjainen tekniikka

VoIP eli IP-puhe on tekniikka, jossa puhe kulkee internet- tai muussa IP-pohjaisessa (Internet Protocol) verkossa. VoIP:ssa äänidata kuljetetaan pakettikytkentäisessä verkossa perinteisen piirikytkentäisen verkon sijaan. VoIP:n toiminta perustuu siis IP-paketteihin ja internet-protokollaan. IP-tekniikan avulla voidaan siirtää puhetta, videota, dataa ym. paketteina samassa tietoväylässä. Tietoliikenteen kehitys onkin menossa siihen suuntaan, että kaikki liikenne kulkee tietoliikenneverkossa IP-paketteina.

IP-tekniikka on halpa ja joustava tekniikka. Tämän takia se on varmasti pitkään verkkojen yleistekniikka. IP-tekniikka on periaatteessa yhtenäinen tekninen alusta eri palveluille. Tieto siirtyy paketeissa sisällön laadusta riippumatta. Siten IP-tekniikka soveltuu hyvin verkkotoimintojen ja palvelutoimintojen eriyttämiseen. IP-tekniikka on tulossa kaikkien operaattoreiden perustekniikaksi nykyisen piirikytkentäisen verkon hävitessä vuosien saatossa. (Haglund & Wirzenius 2005, 5.)

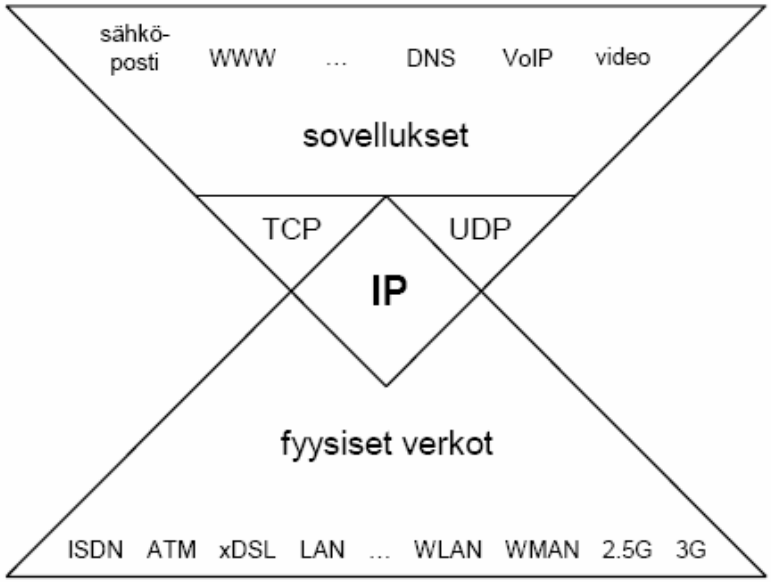
2.2 Internet-verkko

Internet-verkoksi kutsutaan reitittimillä yhdistettyjä paikallisverkkoja, jotka käyttävät IP-protokollaa (Internet Protocol). Internet on tunnetuin internet-verkko. Se on maailman laajin tietokoneverkko, jossa on kymmeniä tuhansia aliverkkoja. Näissä aliverkoissa on kymmeniä miljoonia tietokoneita ja niillä taas satoja miljoonia käyttäjiä.

Internet sai alkunsa 1960-luvulla Yhdysvalloissa, jolloin Yhdysvaltain puolustusministeriön alainen ARPA-toimisto (Advanced Research Projects Agency) kehitti ARPANet-tietoverkon. Internet-verkko kehittyi nykyiseen muotoon 1970-luvulla TCP/IP-protokollan (Transmission Control Protocol / Internet Protocol)

kehittämisen myötä. ARPANET jäi siviilikäyttöön vuonna 1983, ja vuonna 1989 sitä alettiin kutsua nimellä internet. (Karila 2005, 2.)

Jokaisella internetin päätelaitteella on IP-osoite, jonka avulla muut internetin päätelaitteet voivat kommunikoida keskenään. Tiedon siirto tapahtuu IP-paketeissa, joita internetin reitittimet siirtelevät keskenään. IP onkin koko internet-tekniikan ydin, jonka ympärille internet-verkko rakentuu. (Karila 2005, 2.)



KUVIO 1. Internet-arkkitehtuuri (Karila 2005, 2)

Kuvio 1 kuvaa internetin arkkitehtuuria. Nykyisellään internet tarjoaa käyttäjilleen erilaisia palveluja, kuten WWW (World Wide Web), uutisryhmät, tiedostojen siirto, sähköposti ja chat. Internetiin voidaan liittyä lähes minkä tahansa tietoverkon kautta, kuten ISDN (Integrated Services Digital Network), ATM (Asychronous Transfer Mode), xDSL (x Digital Subscriber Line), LAN (Local Area Network), WLAN (Wireless Local Area Network), WiMAX (Worldwide Interoperability for Microwave Access), 2,5G (GSM (Global System for Mobile Communications) / GPRS (General Packet Radio Service) / EDGE (Enhanced Data rates for Global Evolution)) tai 3G (UMTS (Universal Mobile Telecommunications System) ja HSDPA (High-Speed Downlink Packet Access)) (Karila 2005, 2.)

2.3 Internet-protokolla

Voice over IP perustuu nimensä mukaisesti IP- eli internet-protokollaan. IP on yhteydetön protokolla. Se toimii OSI-mallin (Open Systems Interconnection Reference Model) kolmannella eli verkkokerroksella, jossa ei ole käytössä luotettavuusmekanismeja, vuonohjausta tai kuittauksia. Muut protokollat, kuten TCP (Transmission Control Protocol), voivat tarjota nämä ominaisuudet. IP ei myöskään käsittele siirto-ominaisuuksia tai fyysisiä ominaisuuksia. Tämän myötä IP:tä voidaan käyttää virtuaalisesti kaikkialla. Tämä onkin yksi IP:n suurimmista eduista, eli sitä voidaan käyttää lähes missä tahansa verkossa, niin langattomissa, laajakaista- kuin kantataajuusverkoissakin, kotona ja yrityksissä. IP ei myöskään välitä yhteyden nopeudesta eikä laadusta. (Davidson & Peters 2002, 154–155.)

IP-paketin lähetyksessä voidaan käyttää kolmea eri tapaa: yksi- (unicast), moni- (multicast) tai yleislähetystä (broadcast), joista jokaisella on merkittäviä käyttökohteita (Davidson & Peters 2002, 155).

Yksilähetys: Yksilähetys on yksinkertainen. Siinä paketti lähetetään yhteen tiettyyn osoitteeseen. Tämä on yleisin lähetysmuoto, ja siinä kaksi asemaa voi kommunikoida keskenään fyysisestä sijainnista riippumatta. (Davidson & Peters 2002, 155.)

Monilähetys: Monilähetyksessä lähettäjä lähettää yhden paketin, jonka useat tietyt vastaanottajat voivat ottaa vastaan, vaikka ne olisivat eri aliverkossa. Monilähetystä käytetään sovelluksissa, joissa on yksi lähettäjä ja monta vastaanottajaa, mm. videoneuvottelussa. (Davidson & Peters 2002, 155.)

Yleislähetys: Yleislähetyksessä paketit lähetetään saman aliverkon kaikille käyttäjille. Yleislähetys voi kulkea siltojen ja kytkimien läpi, mutta reititin ei välitä sitä eteenpäin, ellei sitä ole määritelty erikseen tekemään niin. (Davidson & Peters 2002, 155.)

3 VOIP:N TEKNIIKAT JA STANDARDIT

3.1 Merkinanto

3.1.1 Perinteisen puhelinverkon merkinanto

Signalointi eli merkinanto määrittelee tavan, jolla puhelu muodostetaan, hallitaan ja puretaan. Puhelun osapuolilla täytyy olla osoitteet, joiden perusteella ne voivat kommunikoida keskenään.

Nykyään yleinen kiinteä puhelinverkko eli PSTN (Public Switched Telephone Network) on maailmanlaajuinen verkko, johon kuuluu noin 750 miljoonaa tilaaja-liittymää eri puolilla maailmaa. Suomessa liittymämäärä on noin 2,8 miljoonaa liittymää. Liittymätiheydeltään Suomi onkin maailman kärkimaita. (Volotinen 1999, 157.) Ennen digitalisoimista analogisia puhelinkeskuksia oli Suomessa yli 5000. Digitalisoimisen myötä määrä on laskenut joihinkin kymmeniin keskuksiin. SDH-tekniikan (Synchronized Digital Hierarchy) ansiosta tiedonsiirtojärjestelmien rakentaminen on niin edullista, että keskuksia on voitu rakentaa entistä harvempaan. (Volotinen 1999, 114.)

Puhelinverkkojen solmupisteet muodostuvat puhelinkeskuksista. Solmupisteet välittävät tulo- ja lähtöjohtojen välistä liikennettä ja siksi niitä kutsutaan välitysjärjestelmiksi. Näitä solmupisteitä yhdistävät siirtojärjestelmät sekä niistä muodostuvat siirtoverkot. TCP/IP-verkkojen (Transmission Control Protocol / Internet Protocol) välitysjärjestelmiä kutsutaan reitittimiksi ja ATM-verkon (Asynchronous Transfer Mode) järjestelmiä kytkimiksi. (Volotinen 1999, 114.)

Puheliikenteen lisäksi puhelinverkkoa käytetään mm. piirikytkentäisessä datasiirrossa. Myös nykyiset xDSL-tekniikat käyttävät hyväkseen nykyistä fyysistä puhelinverkkoa. Puhelinliikenteen suhteellinen osuus pienenee jatkuvasti dataliikenteen vallatessa alaa.

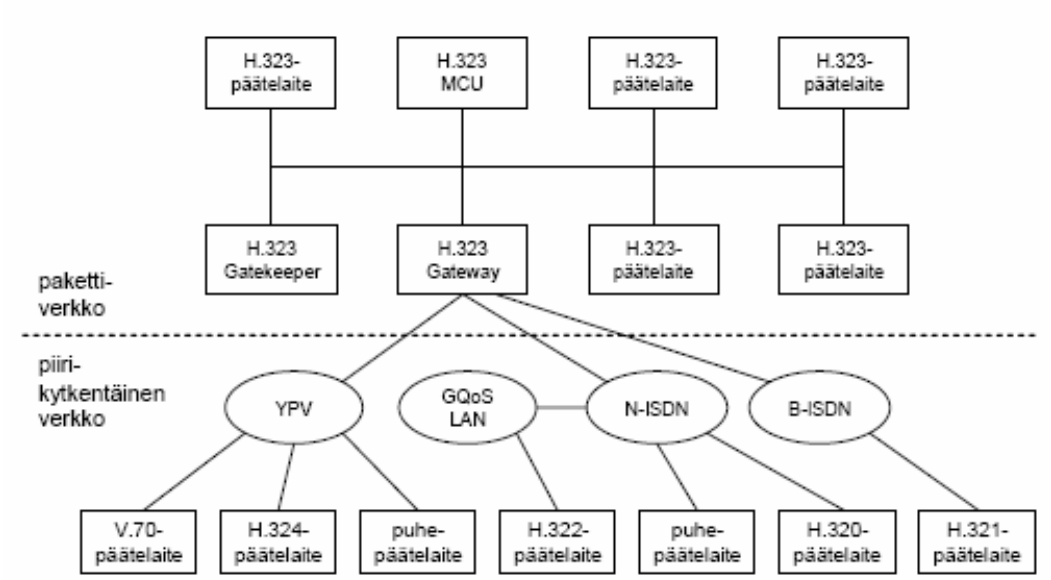
Kun soittaja nostaa kuulokkeen kiinteässä puhelinverkossa, puhelin asettuu korkeaimpedanssiseen tilaan. Päätekeskus havaitsee tämän ja varaa soittajan liittymälle merkinantolaitteen, joka kuuluu soittajalle valintaäänenä. Tämän jälkeen soittaja voi näppäillä puhelinnumeron, jonka puhelinlaite lähettää päätekeskukselle taajuuskoodattuna (DTMF, Dual-tone Multi-Frequency) numero kerrallaan. (Karila 2005, 23.)

Päätekeskus on puhelinkeskus, johon tilaajaverkko on liitettynä. Päätekeskus on liitetty tilaajien lisäksi muutamaan sitä lähinnä olevaan päätekeskukseen ja vähintään yhteen solmukeskukseen. Suomen kaikki päätekeskukset ovat digitaalisia. (Koivisto 1997.) Päätekeskukset kommunikoivat keskenään käyttäen yhteiskanavamerkinantoa. Verkko reitittää kutsutun liittymän päätekeskukselle ja koko reitille varataan piirikytkentäinen 64 kbit/s digitaalinen puhekanava. Vastaanottavassa päässä sijaitseva päätekeskus lähettää kutsutun liittymän tilaajajohtoon korkeajännitteisen soittosignaalin, joka saa puhelimen soimaan. Kun vastaanottaja nostaa kuulokkeen, puhelinkone vaihtaa puhelimen korkeaimpedanssiseen tilaan ja näin päätekeskus saa signaalin, että puheluun on vastattu. (Karila 2005, 23.)

3.1.2 H.323-protokolla

H.323-protokolla on kansainvälisen televiestintäliiton ITU-T:n (International Telecommunication Union Telecommunication Standardization Sector) määrittelemä merkinantoprotokolla. Se on varhaisissa IP-puheluissa käytetty pakettiverkkoprotokolla, joka kehitettiin piirikytkentäisiä videoneuvotteluja varten määritetystä H.320-protokollasta. (Karila 2005, 24.) H.323 määrittää äänen, videon ja datan lähettämisen IP-verkossa. H.323:a on käytetty laajalti VoIP:ssa sekä IP-pohjaisessa videokonferenssijärjestelmissä. (Davidson & Peters 2002, 231.)

H.323:n lähtökohdat ovat perinteisessä puhelinverkossa ja se määrittelee teleoperaattorityyppisen merkinannon. Se yrittää standardoida kokonaisen palvelun ja sen osat. Siksi sitä kutsutaankin sateenvarjostandardiksi, joka määrittelee järjestelmäarkkitehtuurin, puhelunmuodostuksen, hallinnan ja siirtotien. (Karila 2005, 24.)



KUVIO 2. H.323-järjestelmäarkkitehtuuri (Karila 2005, 24)

Kuvio 2 kertoo H.323-stardardin monimuotoisuuden ja samalla havainnollistaa sen ongelmia. Standardi määrittää neljä erilaista komponenttia: päätelaite, MCU (Multipoint Control Unit) eli monipisteneuvottelun hallintayksikkö, portinvartija (Gatekeeper) ja yhdyskäytävä (Gateway), jotka luovat edellytyksen point-to-point- ja point-to-multipoint-palveluille. H.323 määrittelee myös protokollat, jotka tukevat puhelun myöntämistä, aloitusta, tilaa, purkamista ja viestejä H.323-järjestelmissä. (Davidson & Peters 2002, 231–234.)

H.323-arkkitehtuuri on alun perin suunniteltu ympäristöön, jossa liikenne kulkisi piirikytkentäisessä verkossa. Nykyinen kehitys on kuitenkin näyttänyt suunnan, jonka mukaan kaikki liikenne tulee perustumaan pakettikytkentäisyyteen. Tämän myötä H.323:lla ei tule olemaan pitkää tulevaisuutta. (Karila 2005, 25.)

3.1.3 SIP-protokolla

SIP (Session Initiation Protocol) on IETF:n (Internet Engineering Tasking Force) standardisoima, H.323:a nuorempi merkinantoprotokolla. SIP on VoIP:n ydintekniikka ja yleisin käytetty protokolla. SIP-protokollan päätehtävänä on muodostaa,

hallita ja lopettaa istuntoja. SIP perustuu yksinkertaisiin tekstisanomiin, ja tekstipohjaisena se on pitkälti WWW:ssä käytetyn HTTP- (Hypertext Transfer Protocol) ja sähköpostissa käytetyn SMTP-protokollan (Simple Mail Transfer Protocol) kaltainen. (Ericsson 2007; Karila 2005, 25.)

SIP voi käsitellä monentyyppisiä osoitteita, kuten URL- (Uniform Resource Locator), H.323-, E.164- ja sähköpostiosoitteita. OSI-mallin ylimmän eli sovelluskerroksen protokollana se voi käyttää hyväkseen alempien tasojen protokollia, kuten IP:aa, UDP:aa (User Datagram Protocol) ja TCP:aa (Transmission Control Protocol). (Wikipedia 2007.)

SIP:aa käyttämällä voidaan muodostaa puhe-, neuvottelu-, multimedia- sekä muita yhteyksiä internetin yli. SIP:n avulla voidaan muodostaa yksi- tai monilähetysistuntoja sekä point-point- ja multipoint-puheluita. (Davidson & Peters 2002, 235; Karila 2005, 25.) SIP-protokolla ei välitä istunnon laadusta, on kyse sitten puhelusta, videoneuvottelusta tai internet-pelistä. Monikäyttöisyyttä lisää se, että puhelun luonnetta voidaan muuttaa istunnon aikana lisäämällä tai poistamalla käyttäjiä tai medioita. Sähköpostimaisen SIP-osoitteen avulla käyttäjät ovat tavoitettavissa missä päin maailmaa tahansa. (Karila 2005, 25; Westerberg, 5.) SIP käyttää UDP- ja TCP-porttia 5060 (Voip-info.org 2006).

3.1.4 SIP-järjestelmän komponentit

SIP:n toiminta perustuu kahdenlaiseen komponenttiin: käyttäjäagentteihin (User Agent, UA) ja verkkopalvelimiin. Käyttäjäagentit ovat asiakas-palvelinsovelluksia, jotka sisältävät sekä asiakaskäyttäjäagentin, esimerkiksi IP-puhelimen tai PC:n VoIP-ohjelmiston, että palvelinkäyttäjäagentin. Verkkopalvelimia on kolmenlaisia: rekisteröintipalvelimia (Register Server), välityspalvelimia (Proxy Server) tai uudelleenohjauspalvelimia (Redirect Server). (Karila 2005, 26.)

Käyttäjäagentti on päätelaitteessa sijaitseva sovellus, joka toimii vuorovaikutuksessa käyttäjän kanssa. Rekisteröintipalvelin ottaa vastaan sijaintipäivityksiä.

Välityspalvelin toimii muiden asiakkaiden puolesta ja sisältää sekä asiakas- ja palvelintoimintoja. Välityspalvelimen tärkeimpänä tehtävänä on vastaanottaa pyyntöjä ja välittää ne eteenpäin sellaiselle palvelimelle, jolla on tarkempaa tietoa vastaanottajan sijainnista. Käyttäjän päätelaite voi vaihtua, sijaita palomuurin takana ja välillä olla pois päältä tai irti verkosta. SIP-välityspalvelin rekisteröi käyttäjän laitteen ja välityspalvelimen kautta käyttäjä on tavoitettavissa. (Karila 2005, 26.)

3.1.5 SIP:n ominaisuudet ja toiminta

SIP:stä löytyvät multimediaviestintäominaisuudet tekevät siitä tärkeän välineen VoIP:aa ajatellen (Karila 2005, 25; Telecomspace):

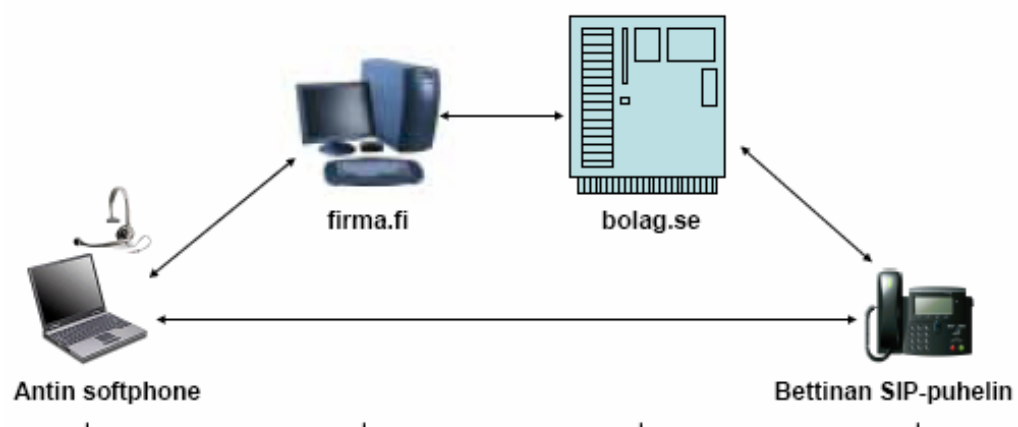
- Käyttäjän sijainti: Tämä ominaisuus mahdollistaa kommunikointiin käytettävän laitteen löytymisen verkosta.
- Käyttäjän tila: Käyttäjä voi määritellä oman sen hetkisen tilansa ja sen myötä olla esim. tuleville puheluille saavutettavissa tai saavuttamattomissa.
- Käyttäjän ominaisuudet: Osapuolet voivat määritellä tuetut ominaisuudet eli mediat, parametrit yms. joita käyttäjän päätelaite tukee.
- Istunnon luominen: Käsittää soittamisen sekä sopimisen osapuolten välillä käytettävistä parametreista.
- Istunnon hallinta: Sisältää istunnon siirron, lopetuksen sekä muutokset.

SIP on ennen kaikkea palveluelementti, jota käytetään yhdessä muiden palveluelementtien kanssa tuottamaan erilaisia palveluita internetin käyttäjille. Internetissä liikenne kulkee IP-paketteina ja monet multimediajärjestelmät perustuvat yhteydettömään UDP-protokollaan. Näiden lisäksi SIP käyttää mm. seuraavia protokollia (Karila 2005, 26):

- RTP (Real-time Transport Protocol): RTP on UDP:n päällä toimiva protokolla, jonka avulla voidaan seurata palvelutasoa sekä siirtää tietoa reaaliaikaisesti. RTP lisää UDP-sanomiin aikaleimat ja järjestysnumerot.
- SDP (Session Description Protocol): Kuvaa multimediaistuntoja. SDP välittää mm. istunnon nimen ja tarkoituksen, käytetyn median, tarvittavat osoitteet, porttinumerot yms. Lisäksi sen mukana kulkee tieto tarvittavasta siirtokapasiteetista ja istunnosta vastaavan henkilön yhteystiedot.
- MEGACO (Media Gateway Control Protocol): Megaco ohjaa yhdyskäytävät yleiseen puhelinverkkoon.

SIP-soittotapahtuman kulku on kuvattu kuviossa 3. SIP:ssä puhelinnumeroa vastaa sähköpostiosoitetta muistuttava SIP-osoite, esim. "sip:antti@firma.fi". Loppuosa "firma.fi" on yrityksen SIP-välityspalvelin, joka rekisteröi Antin käyttäjäagentin. Kun Antti soittaa puhelun Bettinalle, Antin käyttäjäagentti lähettää SIP:n INVITE-viestin omalle SIP-välityspalvelimelleen. Tämä taas lähettää viestin edelleen vastaanottajan eli Bettinan SIP-välityspalvelimelle. Bettinan SIP-välityspalvelin katsoo Bettinan käyttäjäagentin rekisteröimän IP-osoitteen sekä UDP-portin ja lähettää sanoman edelleen Bettinan välityspalvelimelle. Bettinan käyttäjäagentti lähettää OK-viestin, joka kulkee SIP-välityspalvelimien kautta takaisin puhelun soittajalle eli Antille. Antin käyttäjäagentti saa OK-sanoman mukana Bettinan liittymän IP-osoitteen ja porttinumeron, joiden kautta se voi tavoittaa vastaanottajan. Tämän jälkeen Antin käyttäjäagentti lähettää ACK-sanoman Bettinan käyttäjäagentille, eikä puhelun tai puhelun päättämiseen liittyvän merkinannon tarvitse enää kulkea SIP-välityspalvelimien kautta. (Karila 2005, 26.)

Usein käytännössä operaattorit ja palveluntarjoajat kuitenkin kierrättävät puhelun ja signaloinnin omien laitteidensa kautta. Tämä helpottaa palvelutason takaamista, palomuurien läpäisyä ja operaattorien välistä yhdysliikennettä. Signaloinnin kierrättämisen suurin syy on puheluminuuttien seuranta ja laskutus. (Karila 2005, 26.)




```
|                  |                  |                  |
|    INVITE F1     |                  |                  |
|----------------->|    INVITE F2     |                  |
|  100 Trying F3   |----------------->|    INVITE F4     |
|<-----------------|  100 Trying F5   |----------------->|
|                  |<---------------  | 180 Ringing F6   |
|                  | 180 Ringing F7   |<-----------------|
| 180 Ringing F8   |<-----------------|     200 OK F9    |
|<-----------------|    200 OK F10    |<-----------------|
|    200 OK F11    |<-----------------|                  |
|<-----------------|                  |                  |
|                        ACK F12                        |
|------------------------------------------------------>|
|                    media-sessio                       |
|<======================================================>|
|                        BYE F13                        |
|<------------------------------------------------------|
|                       200 OK F14                      |
|------------------------------------------------------>|
|                                                       |
```

```
INVITE sip:bettina@bolag.se SIP/2.0
Via: SIP/2.0/UDP pc33.firma.fi;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bettina <sip:bettina@bolag.se>
From: Antti <sip:antti@firma.fi>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.firma.fi
CSeq: 314159 INVITE
Contact: <sip:bettina@bolag.se>
Content-Type: application/sdp
Content-Length: 142
```

KUVIO 3. Esimerkki SIP-puhelun muodostuksesta, käytöstä ja purusta (Karila 2005, 27)

Kuten kuvio 3 havainnollistaa, puhelun muodostus tapahtuu SIP-välitys-palvelimien kautta. Varsinainen RTP-mediasessio voi sen sijaan tapahtua suoraan osapuolten kesken. Myös puhelun lopettaminen voi tapahtua suoraan. Vaikka SIP on helposti ymmärrettävä merkkipohjainen protokolla, käyttäjät eivät näe

SIP-sanomia, vaan ainoastaan laitteensa käyttöliittymän. Esim. VoIP-puhelin toimii kuten mikä tahansa pöytäpuhelin. (Karila 2005, 27.)

3.1.6 SIP vs. H.323

Molempien edellä esiteltyjen VoIP-protokollien käyttötapa on samankaltainen, niitä voidaan käyttää IP-puheluihin sekä videoneuvotteluun. Vanhemman H.323:n suosion perusta on ollut siinä, että se perustuu enemmän perinteiseen televerkkoajatteluun kuin SIP. Viime vuosien kehitys on kuitenkin selvästi osoittanut, että internet-liikenne tulee perustumaan yhä enemmän IP:aan. Tämän myötä SIP on yleistynyt kovaa vauhtia ja sen odotetaankin jossain vaiheessa syrjäyttävän kokonaan H.323:n. H.323 säilyy kuitenkin vielä joidenkin operaattoreiden järjestelmissä. Onneksi monet VoIP-tuotteet tukevat molempia standardeja ja H.323 sekä SIP on helposti yhdistettävissä toisiinsa yhdyskäytävillä. Uudet VoIP-palvelut kannattaa kuitenkin perustaa SIP:n varaan. (Karila 2005, 28.)

SIP on kaiken kaikkiaan hyvin skaalautuva, yksinkertainen ja kevyt protokolla. SIP:n tärkein ominaisuus on kuitenkin maailmanlaajuinen liitettävyys. Kuka tahansa ympäri maailmaa, joka julkaisee SIP-osoitteensa Internetissä, voi olla kenen tahansa ulottuvilla internetissä. Yhteyteen ei tarvita palveluun kirjautumista, vaan se riittää, että internet-yhteys on saatavissa. (Westerberg, 5.) SIP tukee myös useita puhelinpalveluja. Näiden perustelujen myötä tässä työssä keskitytään merkinnannossa SIP-protokollaan.

3.2 Puheen siirto

3.2.1 Palvelun laatu, QoS

Internet-verkossa kaikki palvelut toimivat IP:n päällä. Jotta puhelu voisi olla laadukas, se tarvitsee riittävästi kapasiteettia. IP-palvelun laatuun vaikuttavat sovelluksen käyttämä kapasiteetti, pakettien viive ja sen vaihtelu sekä pakettien

häviämistodennäköisyys. Se miten UDP-pohjainen VoIP kestää sen, että paketteja häviää matkalla, riippuu käytetystä puheenkoodaustavasta. (Karila 2005, 27.)

DiffServ on internetin palvelunlaatuprotokolla. Se on yhteydetön ja tilaton protokolla eikä DiffServ käytä resurssien varausta, joten se on tehokas ja hyvin skaalautuva. DiffServ on protokolla, jonka mukana kulkee kaikki IP-paketin reitittämiseen tarvittava tieto. Suomalaiset IP-operaattorit ovat käyttäneet DiffServiä intraneteissään jo useita vuosia ja ne ovat tarjonneet sitä myös yrityksille. (Karila 2005, 27.)

IP-pakettien laatuluokituksia on yleensä neljä. Kulta-tasolla (Gold) IP-pakettien viive on erittäin pieni, samoin häviämistodennäköisyys. Luokka sopii hyvin mm. VoIP:lle ja videoneuvottelulle. Hopea-luokassa (Silver) viive on Kulta-luokkaa suurempi, mutta häviämistodennäköisyys on vielä pienempi. Tämä luokka soveltuu hyvin tapahtumakriittisille sovelluksille. Pronssi-luokan (Bronze) viive ja häviämistodennäköisyys ovat pienempiä kuin luokattomalla liikenteellä. Tällainen laatuluokitus sopii hyvin ammattimaiseen WWW-käyttöön. Luokattomassa (Best Effort) palvelussa viive ja häviämistodennäköisyys vaihtelevat suuresti verkon kuormitustilanteen mukaan. (Karila 2005, 27.)

DiffServ sopii erittäin hyvin VoIP-liikenteeseen niin extranetissä kuin internetissäkin. Poliittisena ongelmana tässä kuitenkin nähdään operaattoreiden välinen palvelunlaatureititys, joka ei ole vielä kovin toimiva. (Karila 2005, 27.)

3.2.2 Puheen koodaus

Jotta puhe voidaan siirtää digitaalisena, se pitää digitoida ja koodata. Perinteisessä puhelinverkossa käytetään PCM-koodausta (Pulse Code Modulation). Siinä puheesta otetaan 8 bitin näytteitä 8 kHz:n taajuudella. Näin 4 kHz:n puhekaista muunnetaan digitaaliseksi 64 kbit/s tietovirraksi. VoIP-tekniikassa analoginen signaali muutetaan digitaaliseksi A/D-muuntimella käyttäen käytettävän laitteen,

kuten VoIP-puhelimen, tietokoneen äänikortin tai PC:llä käytettävän VoIP-ohjelman, algoritmia. (Telecomspace 2007.)

Puhetta voidaan tiivistää eli kompressoida niin, että puhe vie vähemmän tilaa ja on tehokkaampaa ilman, että äänenlaatu tästä juurikaan huononee. Kompressointi tapahtuu esimerkiksi äänen taajuusaluetta kaventamalla. Tämän kompressoinnin tekevää algoritmia sanotaan koodekiksi (codec). Koodekit on optimoitu kompressoimaan ääntä, jotka pienentävät merkittävästi kaistanleveyttä verrattuna kompressoimattomaan äänidataan. (Karila 2005, 27; Telecomspace 2007.)

VoIP:ssa käytettävän puheenkoodausmenetelmien tärkeimpiä ominaisuuksia ovat niiden vaatimat siirto- ja prosessointikapasiteetit, niiden aiheuttamat viiveet, algoritmin herkkyys hävinneille paketeille sekä lisenssien ilmaisuus. VoIP:ssa käytetään yleisemmin seuraavia koodekkeja (Karila 2005, 27; Voip-info.org 2006):

- G.711 (PCM) – kompressoimaton, nopeus 64 kbit/s, viive erittäin pieni
- G.723.1 – nopeus 6,3 tai 5,3 kbit/s, jonka yksisuuntainen viive noin 67 ms
- G.726 – nopeus 16/24/32/40 kbit/s, parannettu versio G.721:sta ja G.723:sta
- G.729 – nopeus 8 kbit/s, jonka yksisuuntainen viive noin 25 ms
- iLBC – nopeus 13,3 kbit/s 30 ms tai 15 kbit/s 20 ms kehyksin
- Speex – nopeus 2.15 / 44 kbit/s, käyttää muuttuvaa koodausta.

Näistä iLBC on lisenssivapaa ja sen suosio on nopeassa kasvussa. Se sietää todella hyvin kadonneita ja viivästyneitä IP-sanomia, ja sen vaatima kapasiteetti on vain noin 30 kbit/s. Myös tunnettu Skype-puheohjelma käyttää iLBC:aa puheen koodaukseen. (Karila 2005, 27.)

3.2.3 Reititys

Operaattorit ovat laajasti siirtymässä VoIP:aan, koska se pienentää käyttökustannuksia. Kuitenkin operaattoreiden IP-verkkojen liittäminen yhteen aiheuttaa ongelmia niiden hallinnalle, tietoturvalle ja palvelunlaadulle. (Karila 2005, 33.)

Verkon reunalla sijaitseva SBC (Session Border Controller) on laite, jonka kautta operaattorin yhdysliikenne maailmaan kulkee. SBC:t on suunniteltu helpottamaan reaaliaikaisen multimedian välittämistä verkosta toiseen. Operaattorit ohjaavatkin usemmiten kaiken liikenteen SBC:n kautta helpottaakseen yhdysliikenteen, tietoturvan ja palvelulaadun ylläpitoa IP-verkoissaan. Kun DiffServ saadaan toimimaan, VoIP:n palvelulaadun toteuttaminen onnistuu hyvin myös internetissä. (Karila 2005, 33.)

Nykyisen IPv4 internet-protokollan rinnalle on tullut uusi versio IPv6. Sen käyttö onkin jatkuvasti laajentumassa, koska se mahdollistaa 128-bittisten osoitteiden käytön IPv4:n 32-bittisten sijaan. IPv6 ei ole kuitenkaan vielä levinnyt kovin laajalle USA:ssa ja Länsi-Euroopassa, koska siellä on käytettävissä edelleen melko runsaasti IPv4-osoitteita, mm. NAT:n (Network Address Translation) käytön myötä. Aasiassa ja erityisesti Kiinassa tilanne on toinen, koska koko maahan on varattu IPv4-osoitteita vähemmän kuin yhdelle USA:laiselle yliopistolle. Siksi Kiinassa ja Japanissa uudet VoIP-palvelut kehitetään suoraan IPv6:ta käyttäen. Siirtyminen IPv6:een tuo mukanaan myös muita etuja. Reititystä mm. helpottaa IPv6:ssa käytettävä reititysotsake (Routing Header). Myös IPv6:n IPSec-turvaprotokolla (Internet Protocol Security Architecture) parantaa tietoturvaa. (Karila 2005, 33.)

3.3 Yhdysliikenne

3.3.1 Yhdysliikenne VoIP-järjestelmien välillä

Yhdysliikenne VoIP-järjestelmien välillä on edellytys, jotta IP-puhetta voidaan hyödyntää tehokkaasti. Uusien operaattoreiden käyttämä VoIP peering on

menetelmä, jossa operaattorit liittävät VoIP-järjestelmänsä yhteen vastavuoroisuusperiaatteella ilman keskinäistä laskutusta. (Karila 2005, 35.)

Toistaiseksi uudet operaattorit ovat sopineet peering-järjestelyistä tapauskohtaisesti. Perinteiset operaattorit taas sovittavat VoIP-järjestelmänsä perinteisiin yhdysliikennejärjestelmiinsä. Samalla ne yrittävät soveltaa perinteisiä laskutusmalleja niin pitkään kuin mahdollista. (Karila 2005, 35.)

3.3.2 Yhdysliikenne yleiseen puhelinverkkoon

Toimiva yhdysliikenne VoIP:n ja perinteisen puhelinverkon välillä on yhteisen edun mukaista. ENUM-tekniikka (Telephone Number Mapping) on olennainen osa yhdysliikennettä, siinä puhelinnumerot muunnetaan domain-nimiksi ja tallennetaan internetin nimipalveluun DNS:ään (Domain Name System). (Karila 2005, 35.)

Megaco on protokolla, joka mahdollistaa VoIP-puheluiden kulkemisen pakettivälitteisten IP-verkkojen ja yleisen piirikytkentäisen puhelinverkon välillä (Karila 2005, 35). Suuret tietoliikennealan valmistajat, kuten Siemens ja Ericsson, ovat jo alkaneet käyttää Megaco-protokollaa tulevaisuuden ratkaisuissaan. Joustavana ja monipuolisena protokollana se tarjoaa ratkaisut IP-verkkojen ja yleisen puhelinverkon väliseen yhdysliikenteeseen. (Peltola 2002, 40.)

3.3.3 ENUM – Elektroninen numerointi

ENUM on IETF:n RFC 3761:n mukainen teknologia, jossa E.164-tyyppisestä perinteisestä puhelinnumerosta muodostetaan DNS-järjestelmässä julkaistava internet-osoite eli niin sanottu ENUM-tunnus. ENUM tukee useita palveluita kuten pikaviestit ja sähköposti, mutta ENUM:n tärkein käyttötapa on VoIP-puheluiden ohjaaminen. (Viestintävirasto 2007a.)

ENUM:n avulla on mahdollista soittaa internet-puheluita perinteisellä puhelinnumerolla. Päätelaite muuntaa valitun numeron ENUM-tunnukseksi ja ottaa yhteyden omaan DNS-palvelimeen. Kyselyiden perusteella nimipalvelin lähettää päätelaitteelle puhelun vastaanottajan ENUM-osoitteen. Tämän jälkeen päätelaite kysyy vastaanottajan IP-osoitetta ja näin päätelaite voi ottaa suoraan yhteyttä vastaanottajaan vastauksen saatuaan. (Viestintävirasto 2007a.)

ENUM-muunnoksessa numeroiden järjestys käännetään ja kaikki välimerkit poistetaan. Loppuun lisätään vielä e164.arpa-juuritunnus. Esimerkiksi puhelinnumero ”+358 9 6966 634” voidaan ilmaista verkkotunnuksena ”4.3.6.6.6.9.6.9.8.5.3.e164.arpa”. ENUM-palvelu onkin välttämätön osa puhelinverkon ja internetin välistä yhdysliikennettä. (Viestintävirasto 2007a.)

Suomessa ENUM-palvelua pitää yllä Viestintävirasto, joka aloitti ENUM-tunnusten rekisteröinnin 2.10.2006. Viestintävirasto tarkentaa kuitenkin internet-sivuillaan, että heidän ylläpitämä palvelu ei kuitenkaan palvele loppukäyttäjiä, vaan toimii muiden palvelujen mahdollistajana. Jokainen ENUM-rekisteröinti on tehtävä rekisteröijien kautta, joina toimivat yleensä puhelinyhtiöt ja vastaavat palveluntarjoajat. Vuoden 2007 tammikuuhun mennessä Suomen ainoa rekisteröity ENUM-palveluntarjoaja oli Alajärven Puhelinosuuskunta. (Viestintävirasto 2007a.)

3.4 VoIP:n edut

VoIP on teoriassa vahva kilpailija kiinteälle puhelinpalvelulle. VoIP:n etuna ovat mm. puhelukustannukset, jotka eivät riipu etäisyydestä. Tämän myötä kauko- ja ulkomaanpuheluiden aiheuttama hintalisä saattaa hävitä. Myös paikallispuhelut saattavat muuttua ilmaisiksi, ja erityisesti organisaation sisäverkossa soitetut VoIP-puhelut ovat käytännössä ilmaisia. VoIP-puheluiden hinnanmuodostuksessa kiinnitetään painoarvoa ennemminkin liittymien kuukausimaksuihin ja lisäpalveluihin kuin liikennemääriin. Myös internetin ilmaispuhelupalvelut, kuten Skype,

luovat painetta tähän suuntaan. Mm. näiden seikkojen takia operaattorit tahtovat hidastaa VoIP:n kehitystä. (Haglund & Wirzenius 2005, 8.)

VoIP:n myötä palveluvalikoima lisääntyy ja kustannukset alenevat. Jos palvelut ovat käytettävissä usean operaattorin tarjoamana, ne tarvitsevat standardointia. Palvelujen standardointi on kuitenkin vielä kesken. (Haglund & Wirzenius 2005, 12.)

IP-tekniikasta on tulossa operaattoreiden perustekniikka. Jo nykyään monet pienet kauko-operaattorit käyttävät internetiä ja ne kilpailevat lähes pelkästään hinnalla. Tällainen hintakilpailu pakottaa muut operaattorit laskemaan hintoja. VoIP-ratkaisuilla voidaan ohittaa korkeat kansainvälisen liikenteen terminointimaksut. Tämä lisää kilpailua ja pakottaa laskemaan terminointimaksuja. Suuret kansainväliset operaattorit käyttävätkin jo IP-tekniikkaa kansainvälisillä reiteillä. (Haglund & Wirzenius 2005, 12.)

3.5 EU-lainsäädäntö

EU:n yleispalveludirektiivi on osin yhteensopimaton VoIP-tekniikan kanssa. Muutenkaan VoIP ei näytä sopivan EU:n uusiin sääntelypuitteisiin. Yleispalveludirektiivi on ehkä tekniikkasidonnaisin direktiivi. Syynä on 1990-luvun alun tilanne, jolloin kiinteää puhelintekniikkaa pidettiin tärkeimpänä päätepalveluna. Täten yleispalveludirektiivi on koottu lähinnä perinteisen kiinteän puhelinverkon ominaisuuksien mukaan, osin myös GSM-verkon mukaan. VoIP:n erityispiirteitä ei ole otettu huomioon ja näin direktiivin vaatimukset ovat hyvin vaikea toteuttaa. (Haglund & Wirzenius 2005, 15.)

Vaikuttaa siis siltä, että osin nykyiset, mutta vanhentuneet sääntelyvaatimukset ovat esteenä VoIP:n laajentumiselle. Nykyisiä säätelyvaatimuksia ei tulisi ottaa soveltaa täysin, jos halutaan edistää VoIP-palvelujen käyttöönottoa sekä kiinteän puhelinpalvelun että matkaviestinnän kilpailijana. (Haglund & Wirzenius 2005, 15.)

4 VOIP:N TIETOTURVA

4.1 Tietoturva

Tietoturvallisuus on hyvin laaja käsite. Tietoturvallisuuteen kuuluu yleisesti tietojen synnyttämiseen, käyttämiseen, säilyttämiseen ja hävittämiseen liittyvien laitteiden, ohjelmistojen ja menetelmien sekä henkilöstön muodostama kokonaisuus. Tietoturvallisuuden osa-alueet määrittelee hyvin valtiovarainministeriön tietoturvallisuuden johtoryhmän VAHTIn jaottelu, joka jakaa tietoturvallisuuden kahdeksaan osa-alueeseen (Kerttula 1998, 84-85; Valtiovarainministeriö 2004, 14):

- hallinnollinen turvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoliikenneturvallisuus
- laitteistoturvallisuus
- ohjelmistoturvallisuus
- tietoaineistoturvallisuus
- käyttöturvallisuus.

Tätä VAHTIn mallia on sovellettu myös yksityisellä sektorilla. Yrityksen tai organisaation tietoturvallisuuspolitiikan tulee ottaa huomioon tämän malli. Sitä voidaan soveltaa asettamaan tietoturvallisuudelle omat käytännön tavoitteet ja keinot tavoitteisiin pääsemiseksi. (Kerttula 1998, 84–85)

Tietoturvan perustarpeet ovat seuraavat (Kerttula 1998, 84):

- Luottamuksellisuus (Confidentiality) – tiedot pidetään salassa, eli se on vain niillä, joille se kuuluu.
- Eheys (Integrity) – varmuus siitä, että tieto ei ole muuttunut eikä sitä voi muuttaa ilman lupaa.

- Käytettävyys (Availability) – tiedon tulee olla aina käytettävissä niillä, jotka sitä tarvitsevat ja ovat siihen oikeutettuja.

Nämä ovat tietoturvan ehdottomia perustarpeita. Tietoturvan perustana ovat edellä mainittujen perustarpeiden lisäksi myös seuraavat tarpeet (Kerttula 1998, 84–97):

- Todennus, autenttisuus (Authentication) – menetelmät, joilla voidaan varmistaa osapuolten olevan juuri niitä, joita he väittävät olevansa.
- Kiistämättömyys (Non-repudiation) – vahva todennuksen muoto, jossa tapahtuman jokin osapuoli ei pysty kiistämään olleensa tapahtumassa mukana.
- Pääsynvalvonta (Access Control) – kohdejärjestelmä hallitsee pääsyä tietoihin tai järjestelmään.

Yritykset ja organisaatiot ovat tulleet yhä riippuvaisimmiksi tietoliikenteestä. Sen myötä organisaatio ja yritykset ovat tulleet myös haavoittuvammiksi. Tietojärjestelmien kehityttyä entistä avoimemmiksi näistä tarpeista on tullut hyvin tärkeitä. (Kerttula 1998, 84.)

4.2 VoIP:n kohdistuvat uhkat

Tietoturvallisuuden merkitys tietotekniikassa on jatkuvasti kasvanut. Tietoturva on hyvin olennainen vaatimus tietotekniikan yleistyessä ja ulottuessa kaikenlaisiin sovelluksiin. Tietoturvauhkista puhutaan yhä yleisemmin ja onkin hyvä, että asioista ei olla hiljaa, vaan niitä tuodaan julkisesti esille ja tietoturvaa kehitetään jatkuvasti. VoIP:n tietoturva ei juurikaan ole ollut otsikoissa näihin vuosiin asti, mutta vähitellen VoIP:n yleistyttyä myös sen tietoturva on alkanut kiinnostamaan ja puhuttamaan.

Puhelinjärjestelmän yleisiin tietoturvavaatimuksiin kuuluvat perinteisesti korkea käytettävyys, signaloinnin eheys ja luottamuksellisuus sekä puhelun eheys ja luottamuksellisuus. VoIP:n turvallisuutta voidaan jäsennellä monella tavalla, mutta

usein tietoturvaan sisällytetään seuraavat asiat: eheys, luottamuksellisuus, käytettävyys, palvelunlaatu, merkinanto, virukset, kräkkerit yms. (Karila 2005, 38.)

VoIP perustuu tavanomaisiin palvelimiin, jotka ovat muiden palvelimien tavoin alttiita hyökkäyksille. Palvelimia vastaan kohdistuvat hyökkäykset ovat jatkuvasti kasvaneet ja ne ovat jo arkipäivää. VoIP-palvelimet ovat suosittuja kohteita siinä missä muutkin palvelimet ja ne tulisi suojata kuten muutkin kriittiset palvelimet. Jo nyt on tiedossa tapauksia, jossa VoIP-palvelimiin kohdistuneet verkkomadot ovat kaataneet palvelimia. Tämä on pahimmassa tapauksessa johtanut puhelinpalvelujen pysäyttämiseen. Erityisen vaarallisia ovat DDoS- (Distributed Denial of Service Attacks) eli hajautetut palvelunestohyökkäykset, joita vastaan on vielä vaikea suojautua. (Karila 2005, 38.) Yhdysvaltalaisen SANS-instituutin vuonna 2006 tekemän tutkimuksen mukaan VoIP-palvelimet ja -puhelimet ovat verkkolaitteet-kategoriassa ensimmäisellä sijalla, kun puhutaan potentiaalisista internetin hyökkäyskohteista. Instituutin mukaan monista VoIP-puhelimista ja -järjestelmistä on löytynyt haavoittuvuuksia. Ne voivat johtaa jopa järjestelmän kaatumiseen tai hyökkääjä saattaa saada koko VoIP-järjestelmän hallintaansa. (SANS Institute 2007.)

IP-puhe on kuitenkin pitkälle turvattua, kun sen toteutus tehdään yhtä huolellisesti kuin muutkin kriittiset palvelut. Yrityksissä IP-puheratkaisut on toteutettu edelleen erillisissä osissa. Puhe kulkee sisäverkossa IP-protokollalla, mutta yrityksen ulkopuolella perinteisessä puhelinverkossa. Tämä antaa IP-puheelle lähes yhtä hyvän suojan kuin perinteinen puheratkaisu. (Hämäläinen 2007, 49.)

Tavalliset työasemat toimivat usein puhelinkoneina VoIP-järjestelmissä. Tällaiset työasemat ovat tunnetusti alttiita viruksille, troijalaisille ja muille uhille. Varsinaiset dedikoidut VoIP-puhelimet eivät nekään ole turvassa, vaan niiden sulautetut käyttöjärjestelmät ovat myös alttiita hyökkäyksille. (Karila 2005, 38.)

VoIP:n merkinantokaan ei ole suojassa uhilta. Perinteisessä puhelinverkossa merkinanto kulkee eri kanavassa kuin puhe. VoIP-järjestelmissä kaikki data taas

kulkee IP-verkossa. Tämän myötä VoIP:n merkinanto on herkemmin haavoittuva kuin perinteisen puhelinverkon. (Karila 2005, 38.)

SPIT (Spam over Internet Telephony) on roskapostin vastine VoIP-maailmassa. Se on todellinen uhka, sillä puhelinroskasanomia lähettävät tahot voivat valjastaa automaatteja soittamaan VoIP-numeroihin. Roskasanomat ovat ilmaisia lähettää ja se tekee toiminnasta kannattavaa. (Karila 2005, 38.)

4.3 SIP-protokollan tietoturvauhkat

SIP ei ole helppo protokolla turvata. SIP:n peruskäyttö perustuu elementteihin, joilla ei ole minkäänlaista luottamusta toisiinsa. SIP:n signaloinnin turvallisuudella ei ole merkitystä SIP:n kanssa yhteistyössä käytettävien protokollien, kuten RTP:n, turvallisuuteen. Signaloinnin turvallisuus ei myöskään vaikuta minkään tietyn SIP:n kantavan pääosan kanssa. Mikä tahansa media, joka toimii istunnon kanssa, voidaan salata päästä päähän. Huomioon otettavat turvallisuusuhkat ovat perinteisiä uhkia, jotka tuovat julki SIP:n turvallisuustarpeen. (Rosenberg, Schulzrinne, Camarillo, Johnston, Peterson, Sparks, Handley & Schooler 2002, 233.)

Seuraavaksi tarkastellaan SIP-protokollan tietoturvauhkia. Uhkien lähtökohtana on suojaamaton VoIP-ympäristö, esimerkiksi julkinen internet. Tällaisessa ympäristössä hyökkääjät voivat helposti muokata paketteja, varastaa palveluja, salakuunnella puheluja tai muuten vain häiritä liikennettä. (Rosenberg ym. 2002, 233.)

Rekisteröinnin väärentäminen

SIP-rekisteröinnin toimintatavat antavat käyttäjäagenttien (esim. VoIP-puhelin) tunnistaa itsensä rekisteröintipalvelimelle sellaisena laitteena, josta tietty käyttäjä tavoitetaan. Rekisteröintipalvelin määrittelee rekisteröintiviestin ”From”-kentän perusteella onko vastaanotetulla SIP-pyyntösanomalla oikeus muuttaa yhteysosoitteita. Väärennettyjä rekisteröintejä on melko helppo laatia, koska käyttäjäagentin omistaja voi muuttaa ”From”-kentän tietoa haluamallaan tavalla. Hyökkääjä voi

vaihtaa identiteettinsä ja esiintyä toisena käyttäjänä. Hyökkääjän on mahdollista muuttaa rekisteröintipalvelimella olevia yhteystietoja niin, että tälle käyttäjälle tulevat pyyntösanomat ohjautuvat hyökkääjän omalle laitteelle. Tämä uhka voidaan välttää pääsynhallinnalla. Parhaiten tämä tapahtuu pyyntöjä lähettävän käyttäjäagentin todentamisella. (Rosenberg ym. 2002, 233–234)

Palvelimena esiintyminen

”Request-URI”-kenttä määrittelee yleensä toimialueen, johon käyttäjäagentti lähettää pyyntösanomansa eteenpäin välitettäväksi. On kuitenkin mahdollista, että hyökkääjä voi esiintyä toimialuetta palvelevana palvelimena siepaten nämä pyynnöt. Tällainen tilanne voi syntyä esimerkiksi silloin, kun esim. lahti.com-osoitteeseen lähetetty rekisteröintisanoma siepataan osoitteesta mantsala.com. Hyökkäyspalvelin vastaa kaappaamaansa rekisteröintiin väärennetyllä vastaussanomalla 301 (Moved Permanently). Tällä sanomalla se ohjaa käyttäjäagenttia lähettämään kaikki tulevat käyttäjäsanomat osoitteeseen mantsala.com. Käyttäjäagentti kuitenkin luulee edelleen väärennetyn vastaussanoman tulevan osoitteesta lahti.com. Siksi se noudattaa sanoman mukana tullutta uutta ohjeistusta rekisteröintisanomien suhteen. Jotta tämänkaltainen toiminta voidaan estää, käyttäjäagenttien tulisi käyttää todennusta varmistaakseen vastaanottavan palvelimen oikeellisuuden, ennen pyyntösanomien lähettämistä. (Rosenberg ym. 2002, 234)

Viestirungon peukalointi

Käyttäjäagentit käyttävät pyyntöjen reitittämiseen luotettuja välityspalvelimia. Käyttäjäagentti saattaa antaa välityspalvelimelle luvan ainoastaan reitittää sanomia, mutta ei tutkia tai muuttaa pyyntösanomia. Tämä ei riipu siitä, miten välityspalvelimen luotettavuus on saavutettu. Esimerkiksi voidaan ottaa tapaus, jossa käyttäjäagentti käyttää SIP-sanomarunkoa keskustellessaan mediaistunnossa käytettävistä salausavaimista. Vaikka käyttäjäagentti luottaa toimialueensa välityspalvelimeen merkinannon välittäjänä, sen ei tarvitse antaa lupaa palvelimen pääkäyttäjille purkaa ja tutkia mediaistunnon salattua sisältöä. Vielä pahempi tilanne on,

jos välityspalvelin on valjastettu pahantekoon. Tällöin sen on mahdollista jopa muokata istuntoavaimia tai esiintyä ns. kolmantena miehenä (Man-in-the-middle -hyökkäys). Se saattaa jopa pystyä muuttamaan lähettävän käyttäjäagentin pyytämiä turvallisuuteen liittyviä tunnuksia. Estääkseen tällaiset väärennökset käyttäjäagentti voi salata sanomarungon sekä osan otsikkokentistä päästä-päähän -salauksella. (Rosenberg ym. 2002, 235.)

Istuntojen päättäminen

Kun osapuolten välille on muodostettu yhteys, yhteyden tilaa voidaan muuttaa myöhemmin pyyntösanomilla. Tämän vuoksi osapuolet eivät voi olla varmoja siitä, ovatko pyyntösanomat tulleet toisiltaan vai jostain ulkopuolelta. Esimerkiksi hyökkääjä saattaa pystyä sieppaamaan yhteyden aloitukseen liittyviä sanomia. Näin hyökkääjä saa selville tietoja istunnossa käytettävistä istuntoparametreistä, esim. To ja From. Tämän jälkeen hyökkääjä voi lähettää istuntoon väärennetyn BYE-sanoman. Sanoma näyttää tulevan toiselta yhteysosapuolelta ja istunto päätetään ennenaikaisesti. BYE-sanoman lähettäjän todentaminen on yksi parhaimmista keinoista estää tällainen hyökkäys. Todennuksella voidaan varmistaa, että sanoma on lähtöisin samalta yhteysosapuolelta, jonka kanssa yhteys on perustettu. Sillä voidaan myös estää hyökkääjää saamasta tietoa istuntoparametreista. (Rosenberg ym. 2002, 235–236.)

Palvelunestohyökkäys

Palvelunestohyökkäyksellä (DDoS, Distributed Denial of Service) pyritään halvaannuttamaan jokin tietty tietojärjestelmä tai heikentämään sen käytettävyyttä. Tällainen hyökkäys toteutetaan usein suuntaamalla valtava määrä verkkoliikennettä järjestelmän rajapintoihin. Hajautetulla palvelunestohyökkäyksellä yhden hyökkääjän on mahdollista valjastaa useita koneita käyttöönsä oman koneensa kautta, jotta ne lähettäisivät kohdekoneeseen suuren määrän verkkoliikennettä. Monissa arkkitehtuureissa SIP-välityspalvelimien tarvitsee hyväksyä pyyntöjä maailmanlaajuisista IP-osoitteista. Tämä mahdollistaa palvelunestohyökkäykset ja sen takia

SIP-ylläpitäjien ja järjestelmien kehittäjien tulisi voida tunnistaa ja osoitteellistaa hyökkäykset. (Rosenberg ym. 2002, 236–237.)

4.4 VoIP:n järjestelmätietoturvallisuus

4.4.1 VoIP-järjestelmän turvaaminen

On hyvin todennäköistä, että asemansa vakiinnuttaneet turvaominaisuudet, kuten autentikointi ja salaus, tullaan sisällyttämään VoIP:n standardeihin tulevaisuudessa. Kuitenkin VoIP:n turvallisuuden parantamiseksi voidaan hyödyntää monia olemassa olevia turvatekniikoita jo tänään. Turvallisuuden hallinta VoIP:n verkkotasolla ja IP:n kuljetus- ja verkkotasolla saattaa kuitenkin vaatia verkon uudelleen suunnittelua ja rakentamista. Uudelleen rakentaminen taas saattaa vaikuttaa VoIP-ympäristöä tukevan verkon arkkitehtuuriin. On myös tärkeää muistaa, että minkä tahansa verkon turvaaminen on jatkuva prosessi. Tietoisuus haavoittuvuuksista ja uusimmista ratkaisuista on merkittävässä roolissa. (Defence Information Systems Agency 2006, 31.)

VoIP-ympäristöä tukevan verkon suunnittelu on hyvin tärkeää. Verkkojen täytyy olla rakenteeltaan kestäviä ja eheitä eikä niissä saisi olla heikkoja kohtia. IP-puhetta tukevien verkkojen tulee olla kapasiteetiltaan joustavia. Verkkojen tulee kestää VoIP-liikenteen aiheuttama lisäys nykyiseen tilanteeseen. Lisäksi on otettava huomioon kasvuvara liikenteessä. Verkkojen tulee olla suunniteltu kestämään vikoja tai niiden tulee toipua nopeasti laite- tai verkkovioista. Sähkönsyötön tulee olla turvattu UPS-laitteilla (Uninterruptible Power System). Lisäksi verkossa tulee käyttää palvelun laadun hallintaa. Tässä luvussa tuodaan esille seikat, jotka tulee ottaa huomioon VoIP-ympäristöä pystytettäessä. (Defence Information Systems Agency 2006, 31–33.)

4.4.2 VoIP-palvelimen turvaaminen

Päinvastoin kuin moni tulostinpalvelin tai tavallinen PC, VoIP-palvelin saattaa sisältää erittäin arkaluontoista tietoa. Sen myötä VoIP-palvelin tulee turvata kuten muutkin kriittiset palvelimet. VoIP-palvelimen sijoitus on tärkeää turvallisuuden kannalta. Palvelin tulisi sijoittaa omaan segmenttiinsä, jonka porttina toimii varta vasten VoIP:lle rakennettu palomuuri. Kriittisten VoIP-palvelimien turvaaminen on koko IP-puheympäristön turvallisuuden avain. (Defence Information Systems Agency 2006, 31–33.)

Jotkut palveluntoimittajat toimittavat IP-järjestelmänsä käyttäen omaa käyttöjärjestelmäänsä. Toiset taas käyttävät pohjana UNIX- tai Windows-järjestelmiä. Suurimmat tunnetuimmat uhat kohdistuvat UNIX- ja erityisesti Windows-pohjaisiin järjestelmiin. Näiden järjestelmien ylläpito vaatii erityistä turvaamista. Lisäksi riskien minimoimiseksi näiden palvelimien tulisi toimia ainoastaan VoIP-palvelujen alustana. (Defence Information Systems Agency 2006, 31–33.)

4.4.3 Haavoittuvuuksien hallinta

Haavoittuvuudet ovat nykyään jokapäiväinen ilmiö. Käyttöjärjestelmissä, ohjelmissa ja laitteiden järjestelmissä olevia vähemmän ja enemmän kriittisiä turva-aukkoja löydetään päivittäin. Rikollisissa piireissä näitä aukkoja pyritään hyödyntämään rikollisiin tarkoituksiin ujuttamalle koneelle haittaohjelmia tai pyrkimällä käsiksi koneen tiedostoihin. (Defence Information Systems Agency 2006, 33.)

Haavoittuvuudet koskevat myös IP-puhelinjärjestelmiä. Useimmat järjestelmien ja ohjelmistojen tekijät korjaavat säännöllisesti näitä aukkoja tekemällä paikkoja niihin. VoIP-järjestelmien ylläpitäjien tuleekin jatkuvasti päivittää VoIP-ohjelmistoja ja pitää ne ajan tasalla. On tärkeää, että ylläpitäjät seuraavat aikaansa ja pysyvät ajan tasalla myös tietotaitonsa suhteen. (Defence Information Systems Agency 2006, 33.)

4.5 VoIP:n fyysinen tietoturva

4.5.1 Fyysisen ympäristön turvaaminen

VoIP-ympäristön fyysinen tietoturva on suuri huolenaihe. Reitittimet, kytkimet, yhdyskäytävät ja palvelimet määrittävät VoIP-verkon rajat ja voivat toimia rajapintoina toisiin verkkoihin. Näihin laitteisiin voi perustua koko yrityksen verkon looginen ja fyysinen yhteys ja niitä voidaan pitää mahdollisina hyökkäyskohteina. Jotta fyysinen pääsy näihin laitteisiin voidaan rajoittaa, niiden suojaamiseksi tarvitaan selkeitä toimenpiteitä. Henkilötason fyysisen tietoturvan varotoimenpiteisiin sisältyy mm. rajattu pääsynvalvonta palvelinhuoneeseen ja verkkokaappeihin. Seuraavaksi kuitenkin keskitytään fyysisen tietoturvan tekniseen puoleen. (Defence Information Systems Agency 2006, 34.)

Monista VoIP-laitteista pystyy hakemaan asetukset, joita niihin on määritelty. Tämä helpottaa laitteiden asetusten laittamista ja siitä on apua virhetilanteissa, mutta on vaarallista, jos kuka tahansa pääsee tähän tietoon käsiksi. Esimerkiksi IP-osoitteita voidaan käyttää hyväksi hyökkäyksessä. Siksi kaikkien asetusten tarkastelu tulee olla salasanan takana. (Defence Information Systems Agency 2006, 34.)

Perinteisissä puhelinjärjestelmissä jonkun osan lisääminen järjestelmään vaati yleensä fyysistä johtojen käsittelyä tai muutoksia kytkinten asetuksiin. VoIP:ssa monet järjestelmät toimivat automaattisesti. Nämä järjestelmät saattavat rekisteröidä uuden päätelaitteen automaattisesti puhelunhallintapalvelimelle, kun uusi laite liitetään VoIP-verkkoon. Tämän jälkeen järjestelmä lataa asetukset automaattisesti uuteen laitteeseen. Tämä on tietoturvariski, jos kuka tahansa voi asentaa verkkoon luvatta uuden laitteen tai ottaa sen irti ilman lupaa. Tätä mahdollisuutta voidaan käyttää hyökkäykseen tai tietojen varastamiseen. Automaattirekisteröinti voi tulla kysymykseen suurten VoIP-järjestelmien asennuksessa, mutta muuten muutosten tulisi vaatia manuaalista rekisteröintiä. (Defence Information Systems Agency 2006, 35.)

4.5.2 VoIP- ja dataverkon erottelu

VoIP-verkot ovat yhä suuremmissa määrin arvokas kohde hyökkääjille. Tämän myötä IP-puhe ja sitä tukeva tietoliikenneverkko tulisi turvata mahdollisimman hyvin. Äänen ja datan erottaminen toisistaan parantaa selvästi turvallisuutta ja palveluiden luotettavuutta. Vielä tehokkaampi ratkaisu on ääni- ja dataverkon jakaminen eri verkkoihin. (Defence Information Systems Agency 2006, 36.)

Parhaan turvallisuuden takaamiseksi ääni ja data tulisi jakaa kahteen fyysisesti erilliseen verkkoon samaan tapaan kuten perinteinen puhelinverkko ja tietoliikenneverkko on jaettu. Tällainen ratkaisu saattaa toimia erittäin vaativissa ympäristöissä, mutta se ei ole kovin kustannustehokas tapa rakentaa verkkoa. Looginen VoIP- ja datakomponenttien erotus voidaan tehdä verkkokerroksella VLAN:lla (Virtual Local Area Network) ja kuljetuskerroksella IP-osoitteistuksella. Vaikka näitä metodeja ei ole itsessään suunniteltu turvamekanismeiksi, niillä saavutetaan selvästi lisäturvaa. Lisäksi ne helpottavat suodatuksen hallintaa ja niiden avulla voidaan piilottaa hyökkääjän tarvitsemaa tietoa. Erottamisella voidaan estää myös hyökkäyksen aiheuttamat vaikutukset toiseen verkkoon. (Hämäläinen 2007, 49; Defence Information Systems Agency 2006, 36.)

4.5.3 IP-osoitteiden erottelu

Taulukon 3 mukaisen TCP/IP-viitemallin kolmannen kerroksen erottelu antaa kytkimien, reitittimien ja palomuurien hallita liikennettä pääsylistojen avulla verkon eri komponenttien välillä. Osoitteiden erottelu tapahtuu antamalla VoIP-järjestelmän eri komponenteille erillinen yksityinen IP-verkko tai looginen aliverkko. Reitittämättömiä RFC 1918 -määritelmän mukaisia yksityisosoitteita (10.x.x.x, 172.16.x.x ja 192.168.x.x) tulee käyttää, jos vain mahdollista. Tämä pienentää puheliikenteen pääsyn mahdollisuutta VoIP-verkkosegmentin ulkopuolelle. RFC 1918 -määritelmän mukainen IP-osoiteavaruuden käyttö saa aikaan sen, että ne piilottavat VoIP:n WAN-verkoilta ja estävät yritykset liikennöidä internetiin. (Defence Information Systems Agency 2006, 37.)

TAULUKKO 3. OSI- ja TCP/IP-viitemallit ja niiden kerrokset

OSI	TCP/IP
Sovelluskerros	Sovelluskerros
Esitystapakerros	
Istuntokerros	
Kuljetuskerros	Kuljetuskerros
Verkkokerros	Verkkokerros
Siirtokerros	Siirto- ja fyysinen kerros (peruskerros)
Fyysinen kerros	

4.5.4 VoIP-VLAN

IP-puhelinjärjestelmä rakennetaan IP-infrastruktuurin päälle, joka perustuu TCP/IP-viitemallin 2- ja 3-tason kytkimiin sekä reitittimiin. Nämä sisältävät jakelu- ja liityntäverkon. Turvallinen ratkaisu on se, että puheliikenne eristetään dataliikenteestä käyttäen erillisiä fyysisiä LAN:eja tai virtuaalisia LAN:eja eli VLAN:eja. VLAN:ien käyttö parantaa verkon turvallisuutta, ehkäisee salakuuntelua ja estää muita hyökkäyksiä. (Hämäläinen 2007, 49; Defence Information Systems Agency 2006, 38.)

VLAN:t ovat hyvä ja tehokas tapa jakaa käyttäjät työryhmiin riippumatta fyysisestä sijainnista. Saman VLAN:n asiakkaat voivat viestiä keskenään käyttäen 2-tason kytkentäisyyttä. Ollakseen yhteydessä muihin VLAN:eihin liikenteen tulee kulkea 3-tason laitteen kautta, jonka avulla liikennettä voidaan suodattaa ja reitittää. VLAN:ien avulla IP-puhelinliikenne voidaan erottaa muusta dataliikenteestä. (Defence Information Systems Agency 2006, 38.) Tähän VoIP-VLAN:iin tulisi sijoittaa VoIP-yhdyskäytävät, IP-vaihteet sekä päätelaitteita palveleva VoIP-palvelin. Tämä järjestely takaa myös puheen laadun. (Hämäläinen 2007, 49.)

Tehokkaamman suodatuksen edellyttämiseksi VoIP-laitteet tulisi jakaa loogisiin ryhmiin käyttäen useimpia VLAN:eja. IP-puhelinten tulisi toimia omassa VLAN:ssaan, VoIP-yhdyskäytävät omassaan jne. Tämä järjestely pakottaa 3-tason reitityksen käytön ja reitityksen käyttö taas sallii suodatusominaisuuksien käytön 3-tason laitteissa. Tämän lisäksi jokainen palvelintyyppi tulisi olla omassa VLAN:ssaan. VoIP-laitteet tulisi jakaa seuraavasti (Defence Information Systems Agency 2006, 39):

- VoIP:n DHCP-palvelimet
- hakemistopalvelimet
- viestintäpalvelimet ja palvelimet, joista on liitäntä data- ja VoIP-verkkoon
- yhdyskäytävät
- WAN-liitäntöjen palomuurit
- VoIP-puhelimet, joiden VLAN:it tulisi vielä mahdollisesti jakaa osastoittain tai organisaation mukaan
- työasemat, joissa on ohjelmapohjainen VoIP-puhelin eli ns. softphone
- VoIP-laitteiden hallinta.

Moni IP-puhelin sisältää RJ-45-liitännän tai -liitäntöjä, jotta siihen voi kytkeä työaseman tai muun Ethernet-laitteen. Näiden IP-puhelimien tulisi tukea 802.1Q-standardin mukaista VLAN Trunkingia. VLAN Trunkingilla tarkoitetaan prosessia, jossa monen eri VLAN:n data kuljetetaan eteenpäin yhdessä linkissä. Trunkingilla voidaan eristää puheliikenne muusta liikenteestä, ja se edistää turvallisuutta sekä QoS-ominaisuuksia. Niiden puhelinten, jotka eivät tue 802.1Q VLAN Trunkingia, puhe- ja dataliikenne tulisi yhdistää yhteen VLAN:iin. Sen myötä myös niiden mahdolliset PC-portit tulisi ottaa pois käytöstä. (Defence Information Systems Agency 2006, 39.)

4.5.5 Pääsynhallinta

Sisäverkon suojaaminen luvattomilta käyttäjiltä on tärkeää. Yrityksen työntekijät tai muuten vaan uteliaat voivat päästä helpostikin yrityksen sisäverkkoon. Tämä voi johtaa pääsyyn verkon resursseihin, salakuunteluun tai palvelunestohyökkäykseen yms. VoIP-verkossa. Työaseman tai IP-puhelimen liittäminen suojaamattomaan VoIP-verkkoon voi antaa pääsyn LAN:iin tai puheverkkoon. Tämä kaikki tulee estää. (Defence Information Systems Agency 2006, 40.)

Hyvä keino välttää tunkeilu on liittää kaikki portit, jotka eivät ole käytössä, käyttämättömään VLAN:iin. Tämä estää luvattoman pääsyn VLAN:iin niin fyysisesti kuin loogisestikin. Lisäksi IP-puhelimien käyttämättömät portit tulisi ottaa pois käytöstä, jos niitä ei tarvita. VoIP-päätelaitteen pääsy VoIP-palveluihin tulisi perustua yksilölliseen tarpeeseen ja vain jos päätelaitteella on lupa siihen. Tämä rajoitus merkitsee käytännössä sitä, että ensin tulisi tarkistaa onko ko. laitteella lupa ottaa yhteys verkkoon. Sen jälkeen tulee varmistaa, että laite ohjataan oikeaan VLAN:iin. 2-tason pääsynhallintaan ja VLAN:n ohjaukseen voidaan käyttää seuraavia tapoja (Defence Information Systems Agency 2006, 40):

- Port security -ominaisuus
- porttikohtainen autentikointi 802.1x
- VLAN Management Policy -palvelin (VMPS).

Port security –ominaisuus: Useimmissa kytkimissä on mukana Port security -ominaisuus, jossa käytetään MAC-suodatusta kytkimen portteihin. Tällä ominaisuudella voidaan estää luvattomien laitteiden kytkentä VoIP-verkkoon. Kytkin antaa pääsyn vain niiden laitteiden MAC-osoitteille, jotka on määritelty kytkimen asetuksiin. (Defence Information Systems Agency 2006, 40.)

Porttikohtainen autentikointi 802.1x: 802.1x-standardin tarkoituksena on estää luvattoman asiakaslaitteen pääsy verkkoon lähiverkon liityntäpisteen kautta. 802.1x-tekniikka antaa asiakkaan tunnistautua, autentikoitua ja päästä sisään verkkoon, kun käyttäjä kirjautuu verkkoon. Tämä on kuitenkin vielä harvinainen

ominaisuus IP-puhelimissa ja vasta äskettäin markkinoille on tullut puhelimia, jotka tukevat tätä ominaisuutta. Toisaalta myöskään IP-puhelinta tai IP-puhelimen käyttäjää ei voida autentikoida tällä tekniikalla. (Defence Information Systems Agency 2006, 40.)

VLAN Management Policy -palvelin (VMPS): VMPS on kytkin, joka käyttää laitteen MAC-osoitetta tunnistaakseen laitteen ja pistääkseen tämän oikeaan VLAN:iin. Vaikka MAC-osoitteen väärentäminen on suhteellisen helppoa nykyisillä työkaluilla, on VMPS silti turvallisuutta parantava tekijä. (Defence Information Systems Agency 2006, 40.)

4.5.6 VLAN:ien välinen turvallisuus

VoIP-verkon turvallisuuden parantamiseksi VoIP- ja dataverkon välinen liikenne tulee suodattaa. VoIP-VLAN:ien välinen keskinäinen liikenne tulee myös turvata. Dataverkon liikennettä VoIP-verkkoon päin tulee rajoittaa. Ideaalitilanteessa VoIP- ja data-VLAN:ien välistä liikennettä ei tulisi olla ollenkaan, mutta on tiettyjä tilanteita, joissa se on mahdollista. Esimerkiksi jokin laite data-VLAN:ssa saattaa tarvita pääsyn VoIP-palvelimelle tai jokin VoIP-VLAN:n laite tarvitsee pääsyn data-VLAN:iin. Tällainen liikenne tulisi olla rajoitettu minimiin, mutta on olemassa tilanteita, joissa liikenne voidaan kuitenkin sallia VLAN:ien välillä. Tällainen tilanne syntyy esimerkiksi, kun VoIP:n äänipostipalvelin haluaa olla yhteydessä dataverkon sähköpostipalvelimeen. (Defence Information Systems Agency 2006, 43–44.)

Jos VoIP- ja data-VLAN:ien välillä on dataliikennettä, pakettisuodatus tulee hoitaa sisäisellä palomuurilla tai vähintään 3-tason kytkimien ja reitittimien pääsylistoilla. Näillä keinoilla voidaan rajoittaa portteja ja osoitteita, joille sallitaan pääsy VoIP-VLAN:iin ja VoIP-VLAN:sta. (Defence Information Systems Agency 2006, 44.)

VoIP- ja data-VLAN:in välistä puheliikennettä tulee hallita tilallisella palomuurilla, jossa on ns. tilallinen pakettisuodatus -ominaisuus. Tälläinen palomuuri voi olla dedikoitu sisäinen palomuuri tai se voi olla dedikoidun VoIP-palomuurin lisätoiminto. Tilallisella palomuurilla saavutetaan parempi hallinta ja sen myötä parempi turvallisuus. (Defence Information Systems Agency 2006, 44.)

Eri VLAN:ien välistä liikennettä tulee hallita tilallisen palomuurin tai 3-tason kytkimien ja reitittimien pääsylistoilla. Pääsylistoilla voidaan hallita suunnitellusti VLAN:ien välistä liikennettä. Suodatukessa voidaan sallia IP-puhelimien, yhdyskäytävän, viestipalvelimien yms. välinen liikenne. Liikenne, jossa käytetään portteja ja protokollia ja joita ei käytetä puheenhallintaan tai VoIP:ssa käytettyyn viestintään, voidaan suodattaa pois. (Defence Information Systems Agency 2006, 44.)

4.6 SIP-protokollan turvaaminen

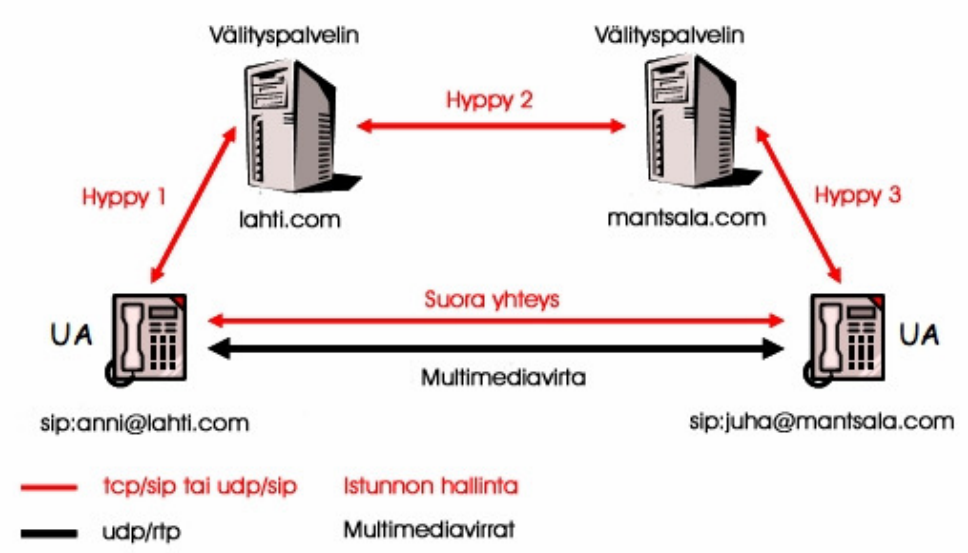
4.6.1 SIP:n tietoturvavaatimukset

Aiemmin lueteltujen SIP:n uhkien perusteella SIP-protokollan perustietoturvavaatimukset ovat seuraavat: sanoman luotettavuuden ja eheyden säilyttäminen, sanomien toistamisen ja väärentämisen ehkäisy, istunnon osapuolien todentaminen ja heidän yksityisyyden suojaaminen sekä palvelunestohyökkäysten estäminen. Lisäksi SIP-sanomien sisältö vaatii erikseen luottamuksellisuus-, eheys- ja todennuspalvelua. Sen sijaan, että SIP-protokollalle määriteltäisiin omat uudet turvamekanismit, SIP:n kanssa tulee käyttää aina kun mahdollista jo olemassa olevia tietoturvamalleja. Nämä mallit tulevat HTTP- ja SMTP-protokollista. (Rosenberg ym. 2002, 237.)

Sanomien täydellisellä salaamisella säilytetään parhaiten merkinannon luottamuksellisuus. SIP-protokollassa itsessään ei kuitenkaan ole mahdollista salata pyyntö- ja vastaussanomia kokonaisuudessaan päästä-päähän-salauksella. Tämä johtuu siitä, että joitain otsikkokenttiä tarvitaan välttämättä sanomien oikeaan reitittämiseen välityspalvelimien kautta. Lisäksi SIP:n toiminta vaatii, että

välityspalvelimien on voitava muuttaa joitain otsikkokenttiä. Tämän vuoksi käyttäjäagenttien on luotettava ainakin jossain määrin käyttämiinsä välityspalvelimiin. Tämän myötä SIP:ssa suositellaan käytettävän alemman tason tietoturvamekanismeja. Nämä mekanismit salaavat pyyntö- ja vastaussanomat kokonaan hyppy-hypyltä-periaatteella (hop-by-hop), ja niiden avulla käyttäjäagentit voivat varmistua välityspalvelimien aitoudesta. Lisäksi SIP:ssa tarvitaan kryptografisia todennusmekanismeja, joilla päätepisteiden välittämät henkilötiedot vastapäiselle käyttäjäagentille tai välityspalvelimelle voidaan tarkistaa oikeiksi. (Rosenberg ym. 2002, 237-238.)

Tyypillinen SIP-istunnon rakenne on selvitetty kuviossa 4. SIP-istunnon parametrit kulkevat yleensä UDP-tietosähkeissä. Ne voidaan kuljettaa myös TCP-streamin mukana, jos käytettävä turvamekanismi vaatii TCP-yhteyttä. Toisaalta mediaistunnoissa käytettävä RTP-protokolla käyttää ainoastaan UDP:a kuljettaakseen ääntä ja kuvaa tosiaikaisesti internetissä. (Steffen, Kaufmann & Stricker 2004, 2.)



KUVIO 4. SIP-istunnon rakenne (Steffen ym. 2004, 3).

Tämä tarkoittaa sitä, että RTP:n kanssa käytettävien turvamekanismien täytyy tukea UDP:a kuljetusprotokollana. Tämän vaatimuksen myötä jotkut tunnetut turvaratkaisut kuten TCP-pohjainen TLS (Transport Layer Security, RFC 2246) eli SSL-salausprotokolla (Secure Sockets Layer), joudutaan jättämään pois

vaihtoehdoista. Seuraavaksi tarkastellaan turvamekanismeja, joita voidaan käyttää taataksemme tiedon eheys ja luotettavuus SIP-istunnoissa ja RTP:n kanssa. (Steffen ym. 2004, 3.)

4.6.2 SIP-istunnon turvaaminen

TAULUKKO 1. Ratkaisuja SIP-viestien turvaamiseksi (Steffen ym. 2004, 4)

Autentikointitavat: **PSK** (Pre Shared Key) **PKI** (Public Key Infrastructure)	Autentikointitapa	Tiedon eheys	Luotettavuus	Muuta tietoa
HTTP 1.0 perusautentikointi	PSK	-	-	Salasanan lähetys ei turvallista
HTTP 1.1 Digest-autentikointi	PSK	-	-	Vastaus-haaste – menettely perustuu vahvan salasanan MD5-tiivisteeseen
PGP (Pretty Good Privacy)	PKI	OK	OK	SIPv2:ssa ei suositella
Secure MIME (S/MIME)	PKI	OK	OK	Vastaanottajan julkinen avain täytyy olla tiedossa salausta varten
SIPS URI (TLS)	PKI	OK	OK	SIP-sovelluksen ja proxyjen täytyy integroitua TLS:ään
IP Security (IPSec)	PKI	OK	OK	Integrointia SIP-sovellusten kanssa ei vaadita, mutta proxyjen pitää olla luotettavia

Koska SIP perustuu tekstipohjaisiin viesteihin HTTP-protokollan tapaan, SIP-istunnon salaamiseen voidaan käyttää hyvin samoja turvamekanismeja kuin HTTP:n suojaamisessa. Näitä ovat mm. myös sähköpostin suojaamisessa käytetyt

PGP (Pretty Good Privacy) tai S/MIME (Secure Multipurpose Internet Mail Extensions). Salattua HTTPS-yhteyttä vastaa SIPS URI (SIP Secure Universal Resource Identifier), joka käyttää TLS:aa suojatun tunnelin rakentamiseksi. Tiedon salaamiseksi voidaan käyttää myös IP Security:a eli IPSec:a. (Internet Protocol Security Architecture, RFC 2401). IPSec:lla voidaan salata kaikenlainen IP-pohjainen liikenne verkkokerroksella. (Steffen ym. 2004, 3.) Nämä turvamekanismit ja niiden käyttämät autentikointitavat on koottu taulukkoon 1.

Taulukon 1 turvamekanismit ovat samat kuin mitä IETF on määrittänyt SIP-standardin versiossa 1. SIP:n versiossa 2 (RFC 3261) sen sijaan ei enää suositella käytettävän HTTP-perusautentikointia eikä PGP:a. (Steffen ym. 2004, 3.)

4.6.3 Kuljetus- ja verkkotason tietoturvamekanismit

Kuljetus- tai verkkotason tietoturvan avulla salataan merkinantoliikenne ja taataan sanomien luottamuksellisuus ja eheys. Alemman tason tietoturva saavutetaan useimmiten sertifikaatteja käyttämällä ja niitä voidaan käyttää myös todennukseen monissa arkkitehtuureissa. (Rosenberg ym. 2002, 238.)

HTTP-perusautentikointi vaatii käyttäjätunnuksen ja salasanan kuljettamista HTTP-pyyntösanoman otsikon mukana. SIP-pyyntösanomaan sisällytettynä SIP-välityspalvelin tai -päätelaite voi käyttää tätä tietoa SIP-asiakkaan tunnistamiseen. Koska selkokielinen salasana voidaan saada helposti selville, tämä on vakava turvallisuusriski. Tämän takia SIPv2-standardissa ei suositella HTTP-perus-autentikoinnin käyttöä. (Steffen ym. 2004, 4.)

HTTP Digest-autentikointi on tilaton, haastepohjainen todennusmekanismi, joka perustuu HTTP-protokollassa käytettyyn todennukseen. HTTP Digest parantaa selvästi perus-autentikoinnin vajavuutta lähettämällä salatun MD5- tai SHA-1-tiivisteen salaisesta salasanasta ja satunnaisesta haasteesta (Steffen ym. 2004, 4). Välityspalvelin ja käyttäjäagentti voivat pyyntösanoman vastaanotettuaan haastaa alkuperäisen lähettäjän hankkimaan varmuuden identiteetistään. SIP:ssa

käyttäjäagentti käyttää 401-vastaussanomaa (Unauthorized) haastaakseen käyttäjäagentin identiteetin. Samaa vastaussanomaa voivat käyttää myös rekisteröintipalvelimet sekä ohjauspalvelimet. Välityspalvelin käyttää haastamiseen 407-vastaussanomia (Proxy Authorization required). Haasteen vastaanottaja uusii lähettämänsä pyynnön ja liittää tarvittavat valtuustiedot joko sanoman ”Authorization”- tai ”Proxy-Authorization”-otsikkokenttään. Jos todennus suoritetaan palvelinkäyttäjäagentille tai rekisteröintipalvelimelle, tiedot sijoitetaan ”Authorization”-kenttään. Välityspalvelimelle todennusta suoritettaessa tiedot sijoitetaan ”Proxy Authorization” -kenttään. Jos valtuustietoja ei ole käytettävissä, käyttäjäagentit voivat yrittää pyynnön uusimista nimettömällä ”anonymous”-käyttäjätunnuksella, ilman salasanaa. (Rosenberg ym. 2002, 193–199.) HTTP Digest -autentikointimenettely edellyttää kuitenkin vahvaa salasanaa, eikä se voi taata luottamuksellisuutta. HTTP Digest ei takaa myöskään SIP-viestin eheyttä. (Steffen ym. 2004, 4.) PGP:a voidaan käyttää tunnistukseen ja SIP-sanomien MIME-hyötykuorman salaamiseen. SIPv2-standardissa ei kuitenkaan suositella PGP:n käyttöä, vaan mieluummin S/MIME:n. (Steffen ym. 2004, 4.)

Kuten edellä on tullut ilmi, SIP:ssa ei ole mahdollista salata koko sanomaa päästä-päähän-salauksella. Verkon välittäjien, kuten välityspalvelinten, tarvitsee lukea tietoa otsikkokentistä voidakseen reitittää viestit oikein. Sähköpostista tuttu Secure MIME eli S/MIME antaa kuitenkin SIP:n käyttäjäagentille mahdollisuuden salata SIP:n MIME-runko päästä-päähän-salauksella. Näin S/MIME:llä voidaan toteuttaa luottamuksellisuus, eheys ja todennus päästä-päähän sanomarungon sisällölle. Lisäksi S/MIME:a käyttämällä on mahdollisuus toteuttaa SIP:n otsikkokentille luottamuksellisuus ja eheys SIP-sanomatunnelin läpi. (Rosenberg ym. 2002, 240.)

S/MIME-toteutusten täytyy tukea vähintään SHA-1:a (Secure Hash Algorithm) digitaalisen allekirjoituksen algoritmina ja 3DES:a salausalgoritmina. Kuviossa 5 on esimerkki salatusta SIP-sanomasta, jossa SDP-runko on salattu S/MIME-salauksella. Asteriskilla (*) merkitty osuus esittää sanoman salattua osuutta. (Rosenberg ym. 2002, 240.)

```
INVITE sip:anni@lahti.com SIP/2.0
Via: SIP/2.0/UDP pc33.mantsala.com;branch=z9hG4bKnashds8
To: Anni <sip:anni@lahti.com>
From: Juha <sip:juha@mantsala.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Contact: <sip:juha@pc33.mantsala.com>
Content-Type: application/pkcs7-mime; smime-
type=enveloped-data;
     name=smime.p7m
Content-Disposition: attachment; filename=smime.p7m
   handling=required

*******************************************************
* Content-Type: application/sdp                       *
*                                                     *
* v=0                                                 *
* o=juha  53655765 2353687637 IN IP4 pc33.mantsala.com*
* s=-                                                 *
* t=0 0                                               *
* c=IN IP4 pc33.mantsala.com                          *
* m=audio 3456 RTP/AVP 0 1 3 99                       *
* a=rtpmap:0 PCMU/8000                                *
*******************************************************
```

KUVIO 5. S/MIME-salattu SIP-sanoma (Rosenberg ym. 2002, 206)

Loppukäyttäjät tunnistetaan sähköpostiosoitteen perusteella, jotka ovat osa SIP URI:a (esim. anni@lahti.com). Tunnistus tapahtuu käyttämällä X.509-varmenteita. Ongelmana X.509:ssa on, ettei loppukäyttäjien varmenteiden myöntäjille löydy maailmanlaajuista luotettavaa tahoa. Omatoimisesti allekirjoitetut varmenteet ovat herkkiä ns. man-in-the-middle-hyökkäyksille. Tämän takia varmenteet tulisi hankkia yleisesti tunnetuilta ja luotetuilta varmenteiden myöntäjiltä. (Steffen ym. 2004, 5.)

Kaksi suosituinta vaihtoehtoa kuljetus- ja verkkotason tietoturvan toteuttamiseksi ovat IPSec ja SIPS URI. IPSec on perinteisen IP-protokollan tietoturvalaajennus, joka koostuu joukosta protokollia. IPSec mahdollistaa IP-sanomien lähettäjän todentamisen, sanoman eheyden varmistamisen sekä tarvittaessa myös kaiken siirrettävän tiedon salauksen. (Rosenberg ym. 2002, 238.) Jokaisen välityspalvelimen täytyy päästä muokkaamaan SIP:n otsikkokenttää ja siksi IPSec:n turvalaajennus ESP (Encapsulation Security Payload) täytyy toteuttaa hyppy-hypyltä-periaatteella (Steffen ym. 2004, 5).

Koska salaus ja todennus tapahtuvat IP-tasolla, kaikki internet-pohjaiset sovellukset voivat käyttää samaa tietoturvamekanismia. IPSec toteutetaan yleensä käyttöjärjestelmätasolla työasemalla. IPSec voidaan toteuttaa myös turvayhteyskäytävällä kuten VPN:lla (Virtual Private Network), joka tarjoaa luottamuksellisuutta ja eheyttä kaikella liikenteelle, jota se ottaa vastaan tietystä rajapinnastaan. (Rosenberg ym. 2002, 238.)

IKE-protokollaa (Internet Key Exchange) käytetään IPSec:ssa hoitamaan avaintenvaihto. IKE tukee sekä PSK- (Pre-Shared Key) että PKI-pohjaisia (Private Key Infrastructure) autentikointiratkaisuja. IKE:n turvayhteyden muodostus perustuu eri vaiheisiin ja ensimmäinen vaihe voidaan suorittaa kahdessa moodissa: päämoodi (Main Mode) ja aggressiivinen moodi (Agressive Mode). Päämoodin ongelma on, että se ei toimi SIP:n käyttäjäagenteille annettujen dynaamisten DHCP-osoitteiden kanssa. Lisäksi myös aggressiivisen moodin kanssa on todettu turvallisuusongelmia. Tämän takia IKE:n kanssa suositellaan käytettävän PKI:a. PKI:n ongelmana saattaa tosin olla luottamuksen puute X.509-sertifikaattien allekirjoittajien todentamiseen, kuten edellä mainitun S/MIME:n kohdalla. (Steffen ym. 2004, 5.)

SIPS URI (TLS) puolestaan tarjoaa kuljetustason tietoturvaa yhteyspohjaisten protokollayhteyksien yli. TLS voidaan määritellä halutuksi kuljetusprotokollaksi ”Via”-otsikkokentän arvolla tai SIPS-URI:llä. TLS sopii parhaiten arkkitehtuureihin, joissa vaaditaan hyppy-hypyltä-salausta sellaisten verkkoisäntien välillä, joilla ei ole aiempaa luottamussuhdetta. Käyttäjäagentilla, joka on lähettänyt pyyntönsä välityspalvelimelle suojatun TLS-yhteyden kautta, ei ole takeita yhteyden suojaamisesta perille asti. Tämä johtuu siitä, että SIP:ssa määritellään kuljetusmekanismit hyppy-hypyltä periaatteella. Mm. tästä syystä TLS tulisi kytkeä tiukasti SIP-sovelluksiin. (Rosenberg ym. 2002, 239.) TLS:n käyttö vaatii TCP:n käyttöä kuljetusprotokollana (TCP/SIP) ja edellyttää PKI-infrastruktuuria. (Steffen ym. 2004, 5.)

SIPS URI:a käyttäen voidaan määritellä, että yhteys asiakaskäyttäjäagentin ja URI:n omistavan toimialueen välillä on suojattu TLS:llä. Tästä eteenpäin

yhteyden suojaamiseen kohdekäyttäjäagentille saakka käytetään ko. toimialueessa määritettyjä tietoturvamekanismeja. (Rosenberg ym. 2002, 148.)

4.7 RTP-protokollan turvaaminen

Multimediavirrat kuljetetaan epäluotettavaa UDP-pohjaista RTP-protokollaa käyttäen. Käytössä on myös RTP:n sisarprotokolla RTPC (Real-Time Transport Protocol), jonka avulla voidaan valvoa pakettivirran luotettavuutta. Valvonnalla voidaan tarkkailla pakettien häviötä ja viivettä. Koska suorat ääni- ja videoyhteydet ovat herkkiä viiveelle ja viiveen vaihteluille, pakettien salauksessa käytettävien menetelmien ei tulisi vaikuttaa näihin arvoihin. Koska RTP:n salausmenetelmien tulee olla UDP-pohjaisia, turvallisuusmekanismeja on vain kaksi. Nämä vaihtoehdot on esitelty taulukossa 2. (Steffen ym. 2004, 6.)

TAULUKKO 2. Ratkaisuja RTP-protokollan turvaamiseksi (Steffen ym. 2004, 6)

Autentikointitavat: **PSK** (Pre Shared Key) **PKI** (Public Key Infrastructure)	Autentikointitapa	Tiedon eheys	Luotettavuus	Muuta tietoa
Secure RTP (SRTP)	PSK	OK	OK	Käyttää ns. master-avainta, joka täytyy jakaa muulla menetelmällä
IP Security (IPSec)	PKI	OK	OK	Integrointia SIP-sovellusten kanssa ei vaadita, mutta asiakkaiden pitää olla luotettavia

Secure RTP eli SRTP on RTP:n laajennus. SRTP:n avulla voidaan toteuttaa RTP- ja RTCP-liikenteen luotettavuus, viestin autentikointi ja toiston suojaaminen. Vahvaksi todetun AES-salauksen (Advanced Encryption Standard) käyttö takaa turvallisuuden, eikä se lisää salatun datan kokoa. Datan eheyden tarkistamiseksi

jokaisen RTP/RTCP-paketin koko kasvaa 10 tavulla. Jos kaista on kapea, tarvittaessa salauksen aiheuttama lisäys voidaan pienentää 4 tavuun. (Steffen ym. 2004, 6.)

IPSec on vaihtoehtoinen salausmenetelmä RTP:lle. IPSec toimii kuten SIP-viestien suojaamisessakin. Vakavaksi ongelmaksi saattaa muodostua ESP-kapsuloinnin aiheuttama pakettikoon muutos. RTP/RTCP-paketin koko saattaa kasvaa 37 tavulla 3DES-salausta käytettäessä. AES:a käytettäessä paketin koko voi kasvaa jopa 53 tavua. (Steffen ym. 2004, 6.)

4.8 VoIP, palomuuri ja NAT

4.8.1 Palomuuri- ja NAT-ongelmat

Sisäverkko tulee suojata kauttaaltaan, jos se on yhteydessä ulkoverkkoon. Tyypillisesti suojaus tapahtuu palomuurilla, erityisesti jos sisäverkosta on yhteys ulkoiseen WAN-verkkoon. Aiemmin mainittujen vaatimusten mukaan ääni- ja dataverkot tulee erottaa toisistaan loogisesti. Jokainen näistä verkoista vaatii erilaisia suojamekanismeja, joka tyypillisesti tarkoittaa erillisiä ääni- ja dataverkon palomuureja. (Defence Information Systems Agency 2006, 46.)

Seuraavat vaatimukset on tarkoitettu VoIP-verkkoa suojaavalle palomuurille, joka suojaa yhteyttä VoIP-verkosta WAN-verkkoon. Jos yhteyttä WAN-verkkoon ei ole, WAN-yhteyttä ei tarvitse suojata ja myöskään palomuuria siinä kohtaa ei vaadita. (Defence Information Systems Agency 2006, 46.)

VoIP itsessään on ongelma verkon turvallisuuden kannalta, mutta myös palomuurit ovat VoIP-järjestelmille ongelma sekä toiminnallisesti että palvelunlaadun kannalta. VoIP-yhteydet ovat suurempi riski sisäverkon tietoturvalle kuin tavanomaiset data-WAN-yhteydet. VoIP-yhteydet ovat erityinen riski sen takia, koska VoIP-yhteydet vaativat, että monen portin pitää olla auki liikenteelle. Syynä on VoIP:n käyttämät protokollat (H.323 ja SIP), jotka käyttävät pakettien kuljettami-

seen todella laajan skaalan (1024-65535) porttinumeroita. (Defence Information Systems Agency 2006, 46.)

Tyypillisesti SIP vaatii neljä porttia yhteyttä kohti, joista kaksi merkinantoa varten. Toiset kaksi vaaditaan mediaa varten, informaation lähettämiseksi ja vastaanottamiseksi. Yhtä puhelua varten muutaman portin avaaminen ei ole varmasti ongelma, mutta kun puheluja on useita, avoimien porttien määrä nousee äkkiä hyvin suureksi. Hyvät pakettisuodattimet pystyvät tarkkailemaan yhteyksien tilaa ja pudottamaan ne paketit, jotka eivät ole osa puhelua. (Defence Information Systems Agency 2006, 46.)

Monet perinteiset palomuurit eivät osaa erottaa sisään tulevaa SIP-liikennettä ja ei-haluttua liikennettä. Tämän seurauksena perinteiset palomuurit saattavat kohdella kaikkea SIP-liikennettä ei-haluttuna liikenteenä ja täten estävät VoIP-liikenteen läpipääsyn yhtiön verkkoon. (Westerberg 2006.) Heikompi palomuuri saattaa estää tulevan äänen läpipääsyn kokonaan. Tuloksena on, että puhelu vaikuttaa yhdistyvän, mutta osapuolet eivät kuule toistensa ääntä. (Newport Networks 2005, 3; Defence Information Systems Agency 2006, 46.)

VoIP-sisäverkossa voidaan ottaa käyttöön osoitteenmuunnos eli NAT. NAT antaa lisäsuojaa VoIP-segmentin ulkopuolisia hakkereita vastaan, koska he eivät voi tutkia VoIP-segmenttiä ja sen haavoittuvuuksia. NAT on kuitenkin ongelma VoIP:n soitonkäynnistuksen ja palvelunlaadun kannalta. Reaaliaikaisena sovelluksena VoIP ottaa yhteyden suoraan käyttäjään IP-osoitteen perusteella, eikä palvelimeen. Koska NAT piilottaa yksityisosoitteet ulospäin, sen käyttö estää VoIP:n toiminnan tehokkaasti. (Defence Information Systems Agency 2006, 46.)

SIP-protokollan vaatima suuri porttimäärä saattaa siis aiheuttaa ongelmia VoIP-verkosta WAN:iin kohdistuvan liikenteen suodatukselle. Tämän takia VoIP:n ja WAN:n välisen palomuurin ominaisuuksista tulisi löytyä tilallinen pakettisuodatus, joka on perinteistä suodatusta kehittyneempi. Lisäksi voidaan käyttää dynaamista eli muuttuvaa porttien mappausta, joka rajoittaa VoIP-liikenteen käyttämien porttien määrää. Dynaaminen porttien mappaus vähentää avoimien porttien

määrää mutta koska jokaista yhteyttä kohti vaaditaan neljä avointa porttia, avoimien porttien määrä voi kasvaa nopeasti suureksi. Dynaaminen porttien mappaus vaatii tilallista palomuuria. (Defence Information Systems Agency 2006, 46–47.)

Staattisella eli pysyvällä mappauksella voidaan asettaa neljä porttia jokaiselle VoIP-yhteydelle. Puhelun asettamisen jälkeen RTP-protokolla käyttää normaalisti vain kahta porttia palomuurin läpi. Staattisen mappauksen konfigurointi vaatii kuitenkin suuren määrän työtä konfiguroida reitittimet oikein. Lisäksi reitittimiä pitää säätää uudelleen joka kerta, kun VoIP:n käyttäjiä halutaan lisätä tai vähentää. Ilman tilallista palomuuria UDP-portteja pitää avata suuri määrä yhteyksien välittämistä varten data- ja VoIP-verkon välillä. (Defence Information Systems Agency 2006, 47.)

4.8.2 Ratkaisuja VoIP:n palomuuri- ja NAT-ongelmiin

Palomuuri- ja NAT-ongelmia ratkaistaan normaalisti ALG:n (Application Level Gateway) ja FCP:n (Firewall Control Proxy) käytöllä. SIP-protokollaa hyvin ymmärtävän ALG:n avulla VoIP-puhelun tarvitsemat portit avataan dynaamisesti yhteyden ajaksi. Jos käytössä on NAT, ALG avaa VoIP-paketit ja muuntaa niiden otsikkotietoja VoIP-sisäverkon IP-osoitteita vastaavaksi. FCP on välityspalvelin, joka antaa ohjeita palomuurille tai NAT:lle. Se tutkii ja tarvittaessa muuttaa SIP-osoitekentän sekä SDP-viestien tietoja. Jos FCP:n vastaanottama data on hyväksyttävää, se antaa palomuurille ohjeen avata ns. neulanreikä paketeille ja näin esimerkiksi äänidata voi kulkea palomuurista tämän reiän läpi. FCP:n avulla voidaan myös parantaa palvelunlaatuongelmia. ALG ja FCP tulee sijoittaa ennen VoIP-palomuuria. Tällä tavalla ne voivat auttaa sekä palomuuria että NAT-sovelluksia hallitsemaan porttien avaamista. (Defence Information Systems Agency 2006, 47.)

NAT:n aiheuttamat ongelmia voidaan ratkaista myös erillisellä STUN-palvelimella (Simple Traversal of UDP through NAT), joka on määritelty RFC 3489:ssa. STUN:n avulla NAT:n takana olevat asiakkaat voivat luoda VoIP-puheluita paikallisen verkon ulkopuolella sijaitsevaan VoIP-palvelimeen.

Asiakkaat saavat STUN-palvelimelta julkisen osoitteen, NAT-laitteen tyypin ja WAN:n puoleisen portin, jonka NAT-reititin on liittänyt paikalliseen porttiin. Näitä tietoja käytetään puhelun luomiseen asiakkaan ja VoIP-palvelimen välillä. (3CX 2007b.)

Liitteessä 1 on lueteltu palvelut ja portit, jotka tulee ottaa huomioon VoIP-palomuurin suodatussääntöjä laatiessa. Jotkut VoIP:n puhelun hallintapalvelimet käyttävät toiminnoissaan yleisesti tunnettuja palveluja, kuten MS-SQL (Microsoft Structured Query Language), NTP (Network Time Protocol), MS:n (Microsoft) päätepalvelut ja HTTP. Ulkomaailmasta tulee estää pääsy näihin palveluihin. (Defence Information Systems Agency 2006, 48.)

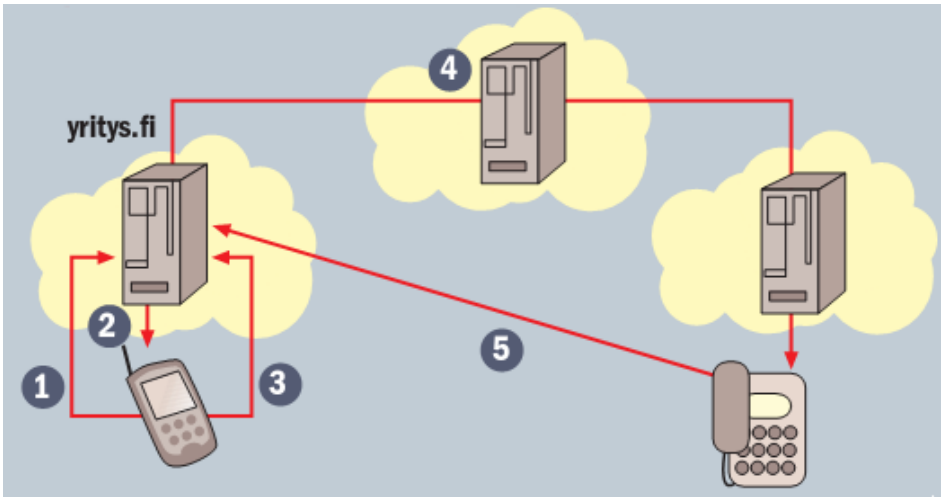
Turvallisuuden takaamiseksi VoIP-palomuurin hallinta tulisi sallia vain sisäverkon liittymästä. Tämä voidaan toteuttaa sisäverkossa paikallisesti tai ulkoa päin turvaprotokollilla kuten SSH (Secure Shell), SNMPv3 (Simple Network Management Protocol version 3), HTTPS tai suojatulla VPN-tunnelilla. (Defence Information Systems Agency 2006, 50.)

4.9 Käyttäjän todennus VoIP:ssa

Vaikka VoIP:n liikenne olisi suojattua ja salattua, soiton aloittaja eli soittaja voi edelleen jäädä tunnistamattomaksi. Tietenkään vastaajankaan identiteetistä ei voida olla varmoja. Jotta VoIP-järjestelmä olisi kauttaaltaan turvallinen, tarvitaan elementti, joka todentaa käyttäjän. (Hämäläinen 2007, 50.)

Salauksen kanssa tarvitaan vahvaa käyttäjän todennusta. SIP URI -osoite on luonteeltaan julkinen tieto, jonka myötä sitä voidaan käyttää esim. SPIT:iin tai väärennettyyn identiteettiin. VoIP-järjestelmä tarvitsee siis menetelmän, joka todentaa soittajan identiteetin. P-Asserted ID (RFC 3325) kehitettiin tätä varten vuonna 2002, mutta se ei allekirjoita tunnistetietoja digitaalisesti. Täten se soveltuu lähinnä vain yritysten intranet-ratkaisuihin. SIP Identity -menetelmällä (RFC 4474)

saatiin tämäkin aukko tukittua. Se toimii varmennepohjaisesti allekirjoittaen tunnistetiedot. (Hämäläinen 2007, 50.)



KUVIO 6. Käyttäjän tunnistus SIP Identity -menetelmällä (Hämäläinen 2007, 50).

Kuviossa 6 kuvataan tapahtumaa, kuinka SIP Identity todentaa soittajan. Todentautumisprosessi etenee seuraavasti: (Hämäläinen 2007, 50.)

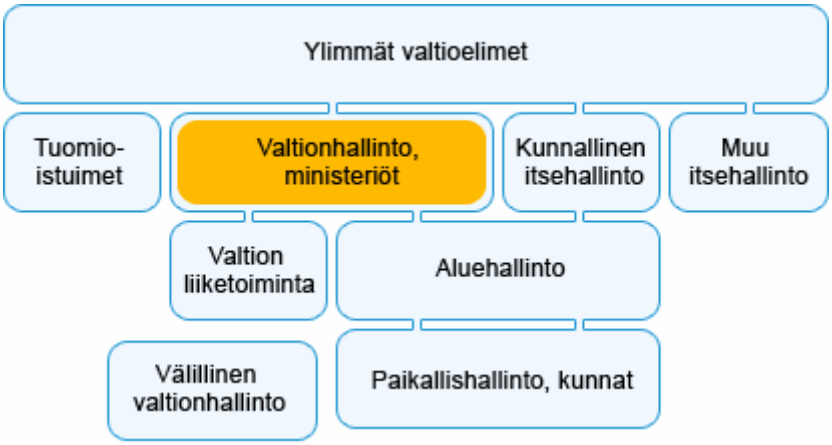
1. Käyttäjä sip:juha@yritys.fi soittaa puhelun.
2. Yritys.fi:n verkon palvelin pyytää Juhan puhelinta tunnistautumaan.
3. Juhan puhelin antaa vastaukseksi valtuustiedot.
4. SIP-palvelin allekirjoittaa SIP-sanoman yksityisellä avaimellaan. Lisäksi se allekirjoittaa sanoman ja lisää URL-osoitteen, josta varmenteen voi hakea.
5. Kutsuttu puhelin hakee varmenteen ja todentaa allekirjoituksen. Tällä tavalla yritys.fi on vahvistanut soittajan olevan Juha.

5 TIETOTURVA JULKISHALLINNOSSA

5.1 Valtion tietoturvallisuus

5.1.1 Julkishallinnon rakenne

Suomen julkishallinto koostuu valtion ylimmistä elimistä ja valtionhallintojärjestelmistä (kuvio 7). Valtionhallintojärjestelmään sisältyy keskushallinto, aluehallinto ja paikallishallinto. Julkiseen hallintoon sisältyy kunnallinen itsehallinto, tuomioistuinlaitos ja valtion liiketoiminta. Julkisen hallinnon tehtävänä on huolehtia yleisestä hallinnosta, järjestyksestä ja turvallisuudesta. Myös hyvinvointipalvelut, kuten koulutus, terveydenhoito ja sosiaalitoimi, kuuluvat sen alaan. (Suomi.fi 2007a.)



KUVIO 7. Suomen julkishallinnon rakenne (Suomi.fi 2007b)

5.1.2 Valtiovarainministeriö vastaa valtion tietoturvallisuudesta

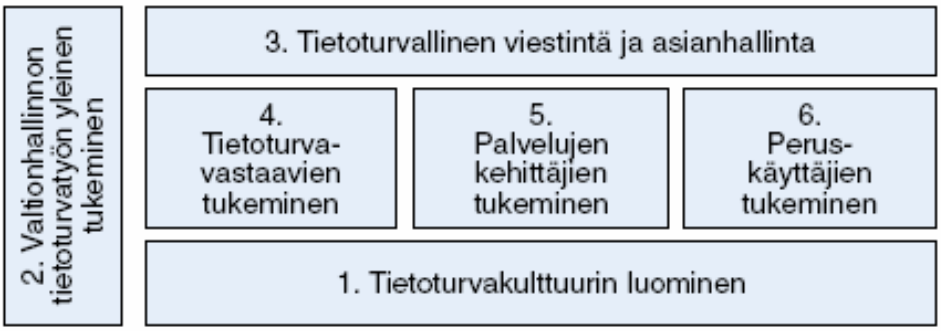
Suomessa on kaksitoista ministeriötä. Ne yhdessä valtioneuvoston kanslian kanssa muodostavat valtioneuvoston eli hallituksen. Hallituksen tehtävänä on toteuttaa eduskunnan säätämät lait ja presidentin päätökset. Käytännössä toimeenpano

tapahtuu kunkin alan ministeriössä. Ministeriöt vastaavat myös toimialoilla olevien virastojen ja laitosten ohjauksesta ja valvonnasta. (Suomi.fi 2007c.)

Valtiovarainministeriö (VM) kuuluu valtioneuvostoon. Ministeriön tehtävän on valmistella hallituksen talous- ja finanssipolitiikkaa ja valtion talousarvion sekä toimii veropolitiikan asiantuntijana. Sen vastuulla on myös rahoitusmarkkinapolitiikan valmistelu, valtion työnantaja- ja henkilöstöpolitiikka sekä julkishallinnon kehittäminen. (Valtiovarainministeriö 2007a.)

Valtiovarainministeriö toimii myös hallituksen asiantuntijayksikkönä hallinnon kehittämistä ja valtion IT-toiminnan ohjausta koskevissa asioissa. Ministeriön tehtävänä on käynnistää hankkeita ja toteuttaa koko hallintoa koskevia kehittämishankkeita, valmistella ja ohjata valtion tietohallinnon ja sähköisten palvelujen yhteisiä asioita. Hallinnon kehittämisen painopisteenä ovat (Valtiovarainministeriö 2007b)

- valtion IT-toiminnan johtaminen ja ohjaus
- sähköiset palvelut ja hallinnon tietoturvallisuus
- julkisten palvelujen tuottavuus ja tuloksenohjauksen terävöittäminen
- palvelujen laatukriteerit ja kansalaisvaikuttaminen hallintoon.



KUVIO 8. Valtion tietoturvallisuuden kehitysohjelma ja sen hankealueet (Valtiovarainministeriö 2006, 5)

Valtion tietoturvallisuuden ohjeistus ja kehittäminen on VM:n vastuulla. Ministeriö on asettanut erityisen Valtiohallinnon tietoturvallisuuden johtoryhmän VAHTIn koordinoimaan valtion tietoturvallisuuden kehitysohjelmaa (kuvio 8), jonka avulla kehitetään tietoturvallisuutta. (Valtiovarainministeriö 2006, 5.)

5.1.3 Valtion tietoturvallisuuden lähtökohdat

Tietoturvallisuus on toteutettava ympäristössä, jossa on toteutettava julkisuutta ja toisaalta turvattava henkilöiden yksityisyyttä ja valtion turvallisuutta. Pääsääntönä on asiakirjan tai sitä vastaavan tiedon julkisuus. Ne tiedot, joiden paljastuminen vaarantaisi keskeisten yksityisten tai julkisten etujen toteutumisen, on salattava ja niiden suojaamisesta on huolehdittava asianmukaisesti. Päätöksenteossa tarvittavan tiedon tulee olla myös viranomaisen käytettävissä. Oikeusturvan kannalta keskeisintä on se, että nämä tiedot ovat samalla oikeita ja asianmukaisia. (Valtiovarainministeriö 2000, 8.)

Suomen laki itsessään asettaa viranomaisille velvoitteen suojata tietojärjestelmät. Keskeinen tietojen suojaamista koskeva säädös on laki viranomaisten toiminnan julkisuudesta (JulkL 621/1999) ja vastaava asetus (JulkA 1030/1999). Julkisuuslain 3 §:ssä kerrotaan, että siinä säädettyjen tiedonsaantioikeuksien ja viranomaisten velvollisuuksien erityisenä tavoitteena on toteuttaa avoimuutta ja hyvää tiedonhallintatapaa. Näitä viranomaisille asetettuja velvoitteita ovat (Valtiovarainministeriö 2000, 8)

- julkisuuden toteutumista palvelevien asialuetteloiden ja tietojärjestelmäkuvausten laatiminen
- tietoon liittyvien oikeuksien kartoittaminen ja huomioon ottaminen
- hyvän julkisuus- ja salassapitorakenteen toteuttaminen asiakirja- ja tietohallinnossa sekä tietojen eheyden ja suojan turvaaminen
- henkilöstön koulutuksesta ja ohjauksesta sekä toiminnan valvonnasta huolehtiminen.

Valtiohallinnon tietoturvallisuuden pohjana oleva koko lainsäädäntö on esitelty liitteessä 2.

5.2 Valtiohallinnon keskeiset tietojärjestelmät

Yhteiskunnan elintärkeät toiminnot on toteutettu keskeisillä tietojärjestelmillä. Verkottuneet järjestelmät muodostavat valtiotasoisen keskeisen tietojärjestelmän, joka on osa valtiohallinnon perusinfrastruktuuria. Valtiohallinnon tietoturvallisuutta ja siihen liittyviä toimenpiteitä ohjaa valtiovarainministeriön hallinnon kehittämisosaston yleisohjaus. Ministeriön asettama tietoturvallisuuden johtoryhmä VAHTI on elin, joka yhteistyössä hallinnon kanssa kehittää ja ohjaa tietoturvallisuutta. (Valtiovarainministeriö 2004, 5.)

VAHTI käsittelee valtionhallinnon tietoturvallisuutta koskevat määräykset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset. Se vastaa myös valtionhallinnon tietoturvaohjeiston kehittämisestä. VAHTIn toimialaan kuuluvat kaikki tietoturvallisuuden osa-alueet: hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineturvallisuus ja käyttöturvallisuus. (Valtiovarainministeriö 2007c.)

Valtion jokaisen viraston on itse riskianalyysien perusteella määriteltävä ne tietojärjestelmät, jotka ovat keskeisiä valtion toiminnan kannalta. Virastot yhtenä kokonaisuutena hoitavat tietoturvallisuuden hallinnoinnin, johon sisältyy tietoturvallisuuden organisointi ja vastuutus. Viraston ylimmän johdon tehtävänä on johtaa tietoturvallisuutta ja sen kehittämistä. VAHTIn ohjeissa tuodaan esille tietoturvallisuuden kehittämisessä huomioitavia säädöksiä, määräyksiä sekä ohjeita. Viraston johdon tehtävänä on vastata siitä, että niitä noudatetaan koko virastossa ja sen toiminnassa. (Valtiovarainministeriö 2004, 5.) VAHTIn julkaisema tietojärjestelmän elinkaaren tietoturvallisuustarkistuslistat löytyvät liitteestä 3.

5.3 Valtiohallinnon tietoliikenneturvallisuusohjeistus

5.3.1 Tietoliikenneturvallisuus

VAHTI määrittelee tietoliikenneturvallisuuden ohjeistuksessaan ne toimet, joilla pyritään aikaansaamaan tietoliikenteen turvallisuus. Turvallisuuteen tähtääviä keinoja ovat mm. laitteistojen ja siirtoyhteyksien ylläpito ja niiden kokoonpanojen hallinta, verkonhallinta, pääsynvalvonta, tietoliikenteen käytön valvonta ja tarkkailu, ongelmatilanteiden kirjaaminen ja selvittäminen, viestinnän salaus ja varmistaminen sekä tietoliikenneohjelmistojen testaus ja hyväksyminen. (Valtiovarainministeriö 2003b, 48.) Valtiohallinnon ohjeistuksessaan VAHTI määrittää mm. IP-puheluille yksiselitteisen vaatimuksen, että puheluiden välittäminen IP-verkoissa on turvattu (Valtiovarainministeriö 2004, 54).

Valtiohallinnon tietoverkon turvallisuus on tärkeää ottaa huomioon jo suunnittelussa. Turvallisuuden lisääminen jälkikäteen ei yleensä auta korjaamaan jos suunnittelussa tehtyjä virheitä. Tietoverkon suunnittelussa on tehtävä tietovirta-analyysi, analyysi turvallisuustavoitteista ja suunniteltava niiden pohjalta tietoverkon turva-arkkitehtuuriratkaisut, turvakomponenttien sijoitteluratkaisut sekä mitoitettava verkon siirtokapasiteetti. Tarvittavien tietoliikenneprotokollien erikoistarpeet tulee myös huomioida. Suunnitteluvaiheen aikana tulee tehdä myös verkon valvonnan suunnittelu ja testaussuunnitelmien laadinta. Suunnittelun pohjana käytetään tietoja, joita siirretään ja niiden turvaluokka. (Valtiovarainministeriö 2004, 55-56.)

Verkon käytettävyysasteen pitämiseksi korkeana, tulee jos suunnitteluvaiheessa ottaa huomioon vaihtoehtoisten tiedonsiirtoreittien ja -resurssien käyttö. Hallinta- ja valvontayhteydet tulee erottaa fyysisesti toisistaan varsinaisessa tuotantoverkossa. Sekä tilaajan että toimittajan velvollisuuksiin kuuluu kaikkien tietoliikenneyhteyksien testaus päästä-päähän. (Valtiovarainministeriö 2004, 56.)

Yrityksen sisäverkko tulee eristää palomuurilla internetistä. Julkiseen ja sisäiseen käyttöön tulevat palvelinlaitteistot tulee myös suojata. Organisaatio voi käyttää

internet-verkkoa omaan sisäiseen tai muiden valtiohallinnon organisaatioiden kanssa käytävään tietoliikenteeseen. Internetin käyttö edellyttää kuitenkin, että organisaatio on ottanut huomioon osapuolten tunnistuksen, tietoliikenteen salauksen ja käytettävyyden vaatimukset. Jos viranomaisen tietojärjestelmät yhdistetään internetin kautta, tulee käyttää vahvaa salausta tai tietoliikenne tulee suojata muilla keinoilla. (Valtiovarainministeriö 2003a, 45.)

Tietoliikenne ja riippuvuus verkoista ovat tärkeitä tekijöitä organisaation toiminnalle. Tästä syystä erityisesti tietoliikenneturvallisuutta tulee painottaa tietoturvallisuuden arvioinnissa. Liitteeseen 4 on esimerkinomaisesti koottu tarkistuslista vaatimuksista, joita voi käyttää julkishallinnossa tietoliikenneturvallisuuden toteutuksessa. Niitä tulee tarkastella esitutkimuksessa teknisinä vaatimuksina. Vaatimusten tavoitteena on ohjata järjestelmien turvalliseen toteutukseen.

5.3.2 Palomuurit ja verkon varmistukset

Palomuuri tulee asentaa tarkan asennussuunnitelman mukaisesti käyttöjärjestelmästä ja protokollapinosta alkaen. Palomuuriin konfiguroitavan sääntökannan tulee toteuttaa tietoliikennepolitiikan mukaiset suodatukset, jotka tulee testata. Kriittisen verkon palomuuri on toteutettava kahdentamalla palomuuri ja siihen liittyvät verkkokomponentit. Kahdennetut verkkokomponentit vaativat huolellista valvontaa. (Valtiovarainministeriö 2004, 57.)

Varmistukset ja varajärjestelyt tulee suhteuttaa kriittisyyden mukaan. Kriittisen verkon tulee olla mahdollisimman vikasietoinen ja turvattu varajärjestelyin siltä varalta, että vikasietoisuus pettää. Varayhteyksien on oltava jatkuvassa käytössä osana tuotantojärjestelmää tai ne on testattava säännöllisin väliajoin. Varajärjestelyjen mitoitus tulee tehdä niin, että ne takaavat riittävän palvelutason. (Valtiovarainministeriö 2004, 57.)

5.3.3 Verkon operointi ja valvonta

Viraston tietoverkolleen laaditussa tietoliikennepolitiikassa tulee dokumentoida mm. sallitut tietoliikenneyhteydet verkkojen välillä, valvonta- ja koestusvälineiden asennus ja käyttö, verkon pääsynvalvonta, verkon käyttö sekä sallitut käyttäjäryhmät. Verkon operointi- ja valvontayhteydet tulee pitää erillään varsinaisesta tuotantoverkosta, mielellään ihan fyysisesti. Operointi- ja valvontajärjestelmät tulee suojata luvattomilta käyttäjiltä sekä kaikki käyttö tulee kirjata lokeihin. (Valtiovarainministeriö 2004, 57.)

Valvonnan tulee kattaa sekä verkon fyysinen valvonta (topologia, komponentit jne.), että liikenteen valvonta (profiili, protokollat jne.). Järjestelmien jotka tekevät fyysistä valvontaa, tulee pystyä havaitsemaan luvattomat laitteet, luvattomat kiinnittäytymiset verkkoon ja näiden yritykset. Liikenteen valvonnan tulee sisältää tunkeutumisen havainnointi- ja estojärjestelmä. Valvonnan tulee havainnoida myös verkon heikentynyt toiminta. (Valtiovarainministeriö 2004, 57.)

Keskeisten järjestelmien käyttämissä tietoverkoissa tulee suosia pysyviä verkko-osoitteita, kuten kiinteät IP-osoitteet tai verkkokorttitunnisteeseen sidottuja dynaamisia IP-osoitteita. Tämä helpottaa vianmääritystä ja sen avulla voidaan helpottaa paikallistamaan poikkeava toiminta. (Valtiovarainministeriö 2004, 58.)

5.3.4 Langattomat tietoliikenneyhteydet

Keskeisten tietojärjestelmien tärkeissä yhteyksissä tulee suosia langallista tiedonsiirtoa. Mikäli kriittinen yhteys on langaton, se tulee turvata langallisella varayhteydellä. (Valtiovarainministeriö 2004, 58.)

Langattomia yhteyksiä käytettäessä todennuksen tulee olla riittävä, koska langattomaan verkkoon voi lähettää dataa kuka tahansa, joka omistaa sopivan lähettimen. Todennuksen taso tulee määrittää riskianalyysin perusteella. Luottamukselli-

nen liikenne tulee myös salata riskianalyysin perusteella, koska langatonta yhteyttä voidaan salakuunnella. (Valtiovarainministeriö 2004, 58.)

5.3.5 Ulkopuoliset yhteydet

Ulkoiset yhteydet ovat aina tietoturvariski. Niiden toteutus tulee tehdä tietoverkolle määritetyn turvallisuus- ja käyttöpolitiikan mukaisesti. Toteutuksen, suojauksen ja valvonnan tulee pohjautua dokumentoituihin riskianalyyseihin. (Valtiovarainministeriö 2004, 58.)

Internet-yhteys tulee toteuttaa siten, että liityntä on suojattu palomuurilla, joka toteuttaa turvallisuus- ja käyttöpolitiikan säännöt. Mahdolliset kumppaniyhteydet voidaan toteuttaa erilaisilla ratkaisuilla, kuten Internet-yhteys, VPN, Frame Relay-yhteys, dedikoitu kaapeli jne. Riskianalyyseillä määritellään yhteyksien salaus-, tunnistus-, todentamis-, käytettävyys- ja eheysratkaisut. (Valtiovarainministeriö 2004, 58.)

Järjestelmien etähuoltoyhteyksille ei tule antaa avointa pääsyä ulkopuolelta. Laitteiston tulisi voida vikatilanteissa ottaa yhteyttä etähuoltoon ja ilmoittaa viasta. Järjestelmävastaava voi sallia ja avata etähuoltoyhteyden huoltoa varten. Etähuollolle tulee määrätä vastuuhenkilö, joka voi valvoa huoltotoimenpiteitä. Huollot suorittava taho on todennettava tietoturvapolitiikan mukaisesti. Pääsy muuhun tietoverkkoon huolto-ohjelmistojen ja -laitteiden kautta on estettävä. (Valtiovarainministeriö 2004, 58–59.)

5.3.6 Verkon eheys, käytettävyys ja luottamuksellisuus

Käytettävyyttä voidaan kasvattaa käyttämällä eri toimittajien tietoturvaratkaisuja samaan tehtävään peräkkäin tai verkon eri pisteissä. Tällä varmistetaan se, ettei yhdessä tuotteessa oleva ongelma vaaranna koko verkkoa. (Valtiovarainministeriö 2004, 59.)

Tiedon eheyden varmistamiseksi lähettäjä tulee todentaa vahvasti. Tietoliikenne tulee toteuttaa sellaisten protokollien avulla, jotka varmistavat tiedon muuttumattomuuden. Todennuksen vahvuus määritellään riskianalyysin perusteella. (Valtiovarainministeriö 2004, 59.)

Luottamuksellisuuden takaamiseksi vastaanottaja tulee todentaa vahvasti. Lisäksi tieto tulee salata tai siirtää dedikoitua, salakuuntelulta suojattua yhteyttä pitkin. Tarvittavien toimenpiteiden taso määritellään riskianalyysin perusteella. (Valtiovarainministeriö 2004, 60.)

5.4 Valtiohallinnon ohjeet IP-puhelinliikennettä varten

Organisaation tietoturvamenettelyissä tulee huomioida erikseen tietoturvavaatimukset, joita edellytetään, jos organisaatioiden välinen tiedonsiirto tapahtuu internetin välityksellä. Tiedonsiirto voi olla sähköposti-, puhe-, tai videoneuvotteluliikennettä. Se voi olla myös tietojärjestelmien etäylläpitoon liittyvää tietoliikennettä. Riippumatta tiedonsiirtotavasta luottamuksellista tietoa ei saa välittää salaamattomana internetin yli. Käyttäjien ja kohteiden tunnistamiseen ja todentamiseen on kiinnitettävä erityistä huomiota. (Valtiovarainministeriö 2003a, 74.)

Jos organisaatio korvaa perinteisen puhelinvaihteen (PBX) IP-puhelinliikenneratkaisulla, viraston tulee huomioida ratkaisun suunnittelussa seuraavat asiat (Valtiovarainministeriö 2003a, 74.):

- IP-puhelinvaihde on palvelin, joka on yhtä haavoittuva kuin mikä muu tahansa palvelin organisaation verkossa.
- IP-puhelinvaihde on suojaamattomana altis viruksille, palvelunestohyökkäyksille ja tunkeutumisille.
- IP-vaihdepalvelin tulisi sijoittaa erilleen muusta lähiverkosta omaan toimialueeseen. Puheliikenne tulisi eristää VLAN:lla ja mahdollisuuksien mukaan puheliikennettä tulisi salata.

5.5 Valtiohallinnon laitteistoturvallisuusohjeistus

Laitteistoturvallisuusohjeistus on tehty toteuttaakseen tietoturvallisuutta tietojenkäsittely- ja tietoliikennelaitteiden ja tilojen käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn ja pääsyn valvontaa sekä varaosien ja tarvikkeiden saatavuuteen liittyviin toimiin (Valtiovarainministeriö 2003b, 23). Palvelinlaitteiden tulee olla valittu vain tähän tarkoitukseen. Laitteet tulee mitoittaa riittäviksi ja ne tulee sijoittaa asianmukaisiin laitetiloihin. Palvelinverkot tulee eristää vaadittavan turvatason ja toiminnallisuuden mukaan. Valvonta-, hallinta- ja varmistusverkot tulee eristää fyysisesti tai loogisesti varsinaisesta tuotantoverkosta. Palvelintilaan tulee olla rajattu pääsy ja palvelimien valvontatilassa tulee olla tiukka pääsynvalvonta. (Valtiovarainministeriö 2004, 64.)

Päätelaitteissa tulee käyttää mahdollisimman pitkälle standardisoituja laitteita. Pääkäyttäjäoikeuksien käyttö tulee olla rajoitettua käyttäjien osalta. Päätelaitteissa tulee käyttää valvontaohjelmistoa, joka lähettää tietoa hallintaan laitteiston ja ohjelmiston kokoonpanosta. (Valtiovarainministeriö 2004, 64.)

5.6 Valtiohallinnnon ohjeet tunnistautumiseen

5.6.1 Yleiset linjaukset

Valtiohallinnon kansalaisille suunnatuissa verkkopalveluissa käyttäjän tunnistamistarve riippuu palvelutyypistä. Kun kyse on tiedottamisesta, käyttäjää ei tarvitse eikä pidäkään tunnistaa. Luottamuksellisessa vuorovaikutteisessa asiointipalvelussa sekä tietojärjestelmien tietojenvaihdossa vaaditaan vahvaa tunnistamista. Kansalaisella ei normaalisti ole pitkäaikaista säännöllistä tarvetta vuorovaikutteiseen asiointiin valtiohallinnon kanssa. Jotta palvelujen käyttö olisi helppoa myös satunnaiselle käyttäjälle, valtion virastojen ja laitosten tulisi välttää omien tunnistautumispalveluiden käyttämistä. VAHTI suosittelee ensisijaisesti tunnistamisessa käytettäväksi valtionhallinnossa hyväksyttäviä vahvoja tunnistamismenetelmiä

tukevia yleisiä tunnistamispalveluja, joita ovat tunnistus.fi sekä VETUMA. (Valtiovarainministeriö 2006, 15.)

Valtiohallinnon sisäisissä, viranomaiskäyttöön tarkoitetuissa verkkopalveluissa käyttäjä tulee aina tunnistaa. Käsiteltävien tietojen luottamuksellisuustaso määrittää tarvittavan tunnistamisen vahvuuden. Tunnistamispalveluita voidaan käyttää myös viranomaispalveluissa, kun se nähdään tarkoituksenmukaiseksi. Valtiovarainministeriö 2006, 15.)
Luotettavuudeltaan parhaimmiksi tunnistamisratkaisuiksi VAHTI pitää laatuvarmenteeseen pohjautuvia PKI-ratkaisuja ja pankkien TUPAS-tunnistautumista. Laatuvarmenteiden toteutusta Suomessa valvoo Viestintävirasto ja pankkien tunnusratkaisuja Rahoitustarkastus. (Valtiovarainministeriö 2006, 15.)

5.6.2 Verkkopalveluiden luokittelu

Verkkopalvelut voidaan jakaa sisällön ja luonteen mukaan seitsemään pääluokkaan. Luokittelu ei ole ehdoton, vaan suuntaa-antava. Sen tarkoitus on helpottaa palveluntarjoajaa tunnistamiselle asetettavan vaatimustason määrittämisessä. (Valtiovarainministeriö 2006, 17.)

- Tietopalvelut ja tiedottaminen – asiakkaalle tarjotaan tietoa hallinnosta.
- Asiakaspalaute ja kansalaisten osallistuminen – kansalaiset voivat antaa palautetta viranomaisille palveluista tai osallistua yhteiskunnan toimintaa kehittävään keskusteluun.
- Ei-luottamuksellinen vuorovaikutteinen asiointi – asiointi koskee muuta kuin asiakkaan luottamuksellisia henkilötietoja.
- Vireillepano – asiakkaan on mahdollista täyttää sähköinen hakemuslomake ja lähettää se viranomaisille sähköisesti.
- Luottamuksellinen vuorovaikutteinen asiointi – asioinnin aikana käsitellään asiakkaan luottamuksellisia henkilökohtaisia tietoja.

- Tietojärjestelmän välinen tietojenvaihto – tietojärjestelmäsovellukset vaihtavat tietoja keskenään, esimerkiksi tietojen haku toisen viranomaisen rekisteristä.
- Viranomaispalvelut – vain viranomaisten sisäiseen käyttöön tarkoitetut verkkopalvelut.

5.6.3 Käyttäjän tunnistamisen luotettavuus

Verkkopalveluissa saavutettavissa olevaa käyttäjien tunnistamisen luotettavuutta voidaan tarkastella kahdella tavalla: Käytetyn identiteetin luotettavuus ja käytetyn käyttäjäidentiteetin todentamisen luotettavuus. (Valtiovarainministeriö 2006, 18.) Käyttäjäidentiteettiin kuuluu palveluntarjoajan tiedossa olevat käyttäjän henkilöllisyyttä kuvaavat tiedot. Käyttäjäidentiteetti luodaan, kun käyttäjä rekisteröidään järjestelmän käyttäjäksi. Identiteetin luotettavuus riippuu täten rekisteröintiprosessista. Jos henkilön tietoja ei tarkisteta mitenkään, käyttäjäidentiteetin luotettavuus on alhainen. Jos henkilöllisyys tarkistetaan luotettavasti kasvotusten, luotettavuus on maksimaalinen. (Valtiovarainministeriö 2006, 18.)

Käyttäjäidentiteetin luotettavuutta voidaan kuvailla seuraavilla luokilla (Valtiovarainministeriö 2006, 18):

- Taso 0: Anonyymikäyttäjät – käyttäjiä ei rekisteröidä.
- Taso 1: Yksilöitävissä olevat käyttäjät – käyttäjät voidaan yksilöidä rekisteröidyn käyttäjäidentiteetin perusteella. Käyttäjäidentiteetti ei välttämättä paljasta käyttäjän todellista henkilöllisyyttä, koska rekisteröinnin yhteydessä käyttäjän antamia tietoja ei ole tarkistettu.
- Taso 2: Kevyesti todennetut käyttäjät – käyttäjillä on käyttäjäidentiteetti, jossa ainakin osa käyttäjän antamista tiedoista on tarkistettu rekisteröinnin yhteydessä. Täten käyttäjäidentiteettiä voidaan pitää moneen tarkoitukseen luotettavana.

- Taso 3: Vahvasti todennetut käyttäjät – käyttäjien henkilöllisyys on selvitetty luotettavasti ja henkilö on todistanut henkilöllisyytensä henkilökortilla, ajokortilla tai passilla. Henkilön identiteetin on varmistanut valtuutetun organisaation edustaja.

5.6.4 Käyttäjän todentamisen luotettavuus

Todentamisen luotettavuus riippuu tunnistamisessa valitusta todentamismenetelmästä. Käyttäjäidentiteetin todentaminen perustuu johonkin seuraavista vaihtoehdoista (Valtiovarainministeriö 2006, 20):

- Johonkin mitä käyttäjä tietää. Tämä on eniten käytetty todentamistapa sähköisessä asioinnissa. Se tarkoittaa salasanaa tai salalausetta, jonka käyttäjä joutuu antamaan käyttäjätunnuksen yhteydessä.
- Johonkin mitä käyttäjällä on. Tässä on kyse välineestä, jolla käyttäjä voi tunnistautua. Välineitä voivat olla esimerkiksi sirukortti tai tietyllä SIM-kortilla varustettu matkapuhelin.
- Johonkin mitä käyttäjä on. Tällä tarkoitetaan käyttäjän biometristä ominaisuutta. Käyttäjä voidaan todentaa esimerkiksi sormenjäljestä, kasvojen muodosta, silmän iiriksestä tai äänestä.

Kyse on kevyestä tunnistamisesta, jos käytössä on vain yksi tunnistamistapa edellä mainituista. Esimerkki tästä on käyttäjätunnus + salasana tai pelkkä sormenjälkitunnistus. (Valtiovarainministeriö 2006, 20.) Käyttäjätunnus ja salasana ovat perinteisesti riittäneet käyttäjän tunnistamiseen ja todentamiseen suljetuissa järjestelmissä. Myös internetissä salasanan suojaus on mahdollista turvata salauksella, jolloin sitä voidaan käyttää rekisteröityjen käyttäjien todentamiseen. (Valtiovarainministeriö 2003a, 30)

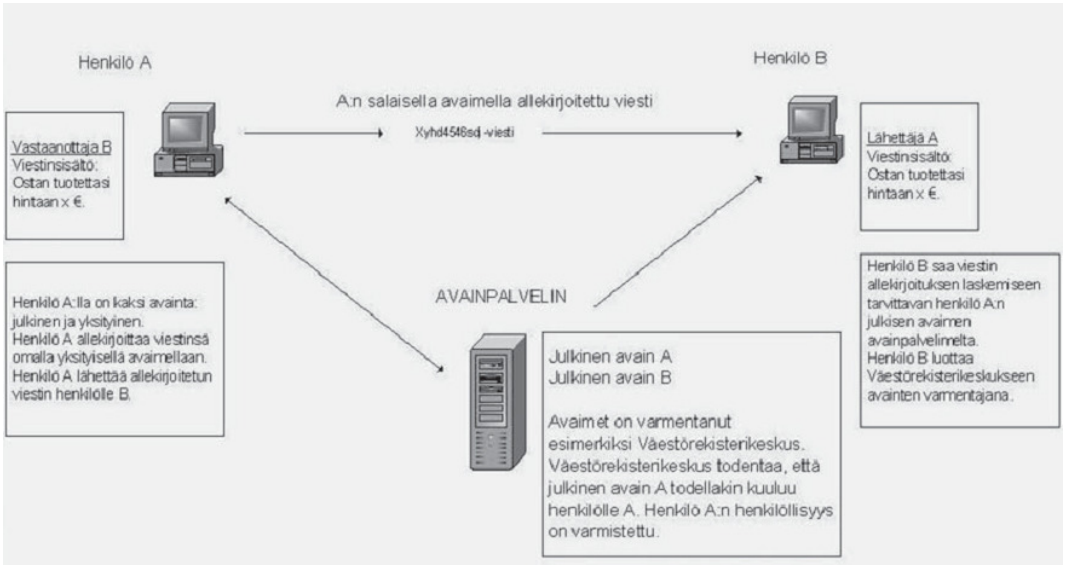
Vahvassa tunnistamisessa käytetään kahta tunnistamistapaa. Tällainen tunnistamismenetelmä on esimerkiksi verkkopankkitunnuksiin ja vaihtuvaan salasanalistaan perustuva TUPAS-tunnistus. Myös varmenteellinen sirukortti + salasana tai

varmenteellinen sirukortti + biotunnistus ovat vahvoja tunnistamistapoja. (Valtiovarainministeriö 2006, 20.) Tietoturvallisuuden kannalta suositeltavin ratkaisu on laatuvarmenteen kriteerit täyttävä toimikortti-PIN-yhdistelmä (Valtiovarainministeriö 2003a, 30).

5.6.5 PKI-infrastruktuuri

Tietoyhteiskunnassa edellytetään turvallisia ja luotettavia palveluja ja sovelluksia. Tähän tarvitaan luotettuja kolmansia osapuolia (TTP, Trusted Third Party) ja heidän tarjoamiaan palveluita. TTP-palvelut rakentuvat pääsääntöisesti julkisen avaimen järjestelmän eli PKI:n (Public Key Infrastructure) päälle. (Kerttula 1998, 327.)

Luotettava viestintä perustuu autenttisuuteen (aitous) ja tietosuojaan (salaus). Ne ovatkin PKI- ja TTP-palveluiden perustana. Julkisen avaimen salauksessa tieto salataan vastaanottajan julkisella avaimella ja puretaan vastaanottajan salaisella avaimella. Samaa algoritmia käytetään myös käänteisesti eli tieto salataan omalla salaisella avaimella ja se voidaan purkaa saman henkilön julkisella avaimella. Salattu tieto toimii digitaalisena allekirjoituksena. Salaisen avaimen ja samalla myös digitaalisen allekirjoituksen autenttisuus varmennetaan luotettavan kolmannen osapuolen antamalla sertifikaatilla eli varmenteella. Luotettu kolmas osapuoli varmistaa käyttäjän varmenteen, jolloin voidaan varmistua, että varmenne kuuluu kyseiselle henkilölle. Kuvio 9 antaa esimerkin PKI-järjestelmän toimivuudesta. (Kerttula 1998, 332.)



KUVIO 9. Esimerkki viestin alkuperän todentamisesta PKI-järjestelmässä (Valtiovarainministeriö 2003a, 32)

Julkisen avaimen järjestelmällä voidaan taata myös tapahtuman kiistämättömyys. Kiistämättömyyteen tarvitaan sähköinen allekirjoitus, jossa yksityisellä avaimella allekirjoitetaan (datasta luodaan tiiviste). Tällöin vastaanottaja varmistaa laskemalla tiivisteen uudelleen lähettäjän julkisella avaimella olevien tietojen avulla. Sen jälkeen vastaanottaja vertaa tiivistettä alkuperäiseen tiivisteeseen varmistuakseen, että varmenne oli oikea. (Valtiovarainministeriö 2003a, 31.)

Laatuvarmenteiden käyttöä valvoo Viestintävirasto. Tällä hetkellä ainoa laatuvarmenteiden tarjoaja Suomessa on Väestörekisterikeskus. (Valtiovarainministeriö 2003a, 31.)

Suljetussa verkossa oleva yksittäinen palvelinlaite voidaan tunnistaa IPSec-menetelmällä. IP-Sec-suojausta käytettäessä verkon ylläpitäjä allekirjoittaa jokaisen laitteet julkisen avaimen omalla yksityisellä avaimellaan. Tämän jälkeen jokaisella verkossa olevalla laitteella on hallussaan (Valtiovarainministeriö 2003a, 33.)

- laitteen oma yksityinen avain
- laitteen julkinen avain

- ylläpitäjän allekirjoittama laitteen julkisen avaimen varmenne
- ylläpitäjän julkinen avain.

Kun verkon laitteet ovat yhteyksissä keskenään, ne antavat yhteyskumppaneilleen oman julkisen avaimensa ja varmenteensa. Samalla ne tarkistavat vastapuolelta saamansa varmenteen allekirjoituksen. Seuraavaksi kumpikin osapuoli varmistaa, että toisella osapuolella on hallussa julkista avainta vastaava yksityinen avain. Näin osapuolet voivat luottaa toisiinsa ja vaihtaa salattua tietoa. (Valtiovarainministeriö 2003a, 33.)

5.7 Viestintäviraston määräykset operaattoreille

5.7.1 Viestintävirasto valvoo teleyritysten tietoturvallisuutta

Suomessa ei ole yhtenäistä tietoturvallisuuslainsäädäntöä, vaan säännöksiä sisältyy useisiin lakeihin ja asetuksiin. Sähköisen viestinnän tietosuojalain (SVTsL, 516/2004) noudattamista valvoo Viestintävirasto. Osan valvontatehtävistä hoitaa tietosuojavaltuutettu. Viestintäviraston valvoma viestintämarkkinalaki (393/2003) sisältää teleyrityksiä koskevan yleisen tason tietoturvallisuusvelvoitteen. Viestintävirasto valvoo myös sähköisen viestinnän tietosuojalain ja viestintämarkkinalain nojalla annettujen säännösten ja määräysten noudattamista. (Viestintävirasto 2007b.)

Viestintävirasto määrittelee teleyritysten tietoturvan määräyksessään teleyritysten tietoturvasta (47 B/2004 M). Määräykseen on kirjattu vaatimuksia, jotka koskevat hallinnollista turvallisuutta, henkilöstöturvallisuutta, tietoliikenneturvallisuutta, laitteisto- ja ohjelmistoturvallisuutta, tietoaineistoturvallisuutta ja käyttöturvallisuutta. Määräystä tulee soveltaa teleyritysten yleisten viestintäpalvelujen toteuttamisen liittyvään toimintaan sekä teleyritysten yleiseen toimintaan ja sen käyttämiin järjestelmiin, viestintäverkkoihin ja -palveluihin. (47 B/2004 M 2 - 7§.)

5.7.2 Sähköposti- ja internet-yhteyspalvelujen tietoturvamääräykset

Viestintäviraston määräys sähköpostipalvelujen tietoturvasta ja toimivuudesta (11/2004 M) velvoittaa teleyrityksen huolehtimaan sähköpostijärjestelmistään. Määräys velvoittaa teleyrityksen seuraamaan oman viestintäverkkonsa ja sähköpostijärjestelmän tapahtumia, jotta verkolle tai palvelulle vaaraa aiheuttavat haittaohjelmat voidaan havaita. Tarvittaessa teleyritys on velvollinen kytkemään irti yleisestä viestintäverkosta tietojärjestelmän tai liittymän, jos se on tarpeen tietoturvan tai käytettävyyden huolehtimiseksi ja tietoturvan tai käytettävyyden lisäämiseksi.

Viestintäviraston määräys internet-yhteyspalvelujen tietoturvasta ja toimivuudesta (13/2005 M) määrää teleyrityksen suorittamaan asiakasliittymiä koskevat toteutus- ja ylläpitotoimenpiteet tietoturvanäkökohdat huomioon ottaen. Teleyrityksen on erotettava tilaajien liikenne toisistaan niin, että tilaajat eivät oikeudettomasti voi seurata toistensa liikennettä. Määräyksen mukaan teleyrityksen on määriteltävä sekä kuvattava asiakkaalle asiakasliittymän osalta selkeät käyttösäännöt. Niihin sisältyy liittymän käyttöön vaikuttavat tekniset rajoitukset, kuten tietoliikenneporteihin, -protokolliin tai liikennemääriin vaikuttavat rajoitukset. Teleyrityksen on myös suodatettava sellainen asiakasliittymästä lähtevä liikenne, jonka lähdeosoite ei ole kyseiselle asiakasliittymälle osoitettu. (13/2005 M, 3 - 4§.)

Määräyksen 5. pykälässä määritellään haitallisen liikenteen havaitseminen ja suodattaminen asiakasliittymissä. Sen mukaan teleyrityksen on seurattava omaa viestintäverkkoaan vaaraa aiheuttavan liikenteen havaitsemiseksi. Asiakasliittymien liikenteen tilapäiseksi suodattamiseksi tulee löytyä toimintamallit. Jos viestintäpalvelun tietoturva tai käytettävyys vaarantuu oleellisesti, teleyrityksen on kytkettävä asiakasliittymä tai sen palvelu irti. (13/2005 M, 5§.)

Teleyritykseltä täytyy löytyä ohjeet ja toimintamallit palvelunestohyökkäystilanteiden tai muiden tietoturvaa tai käytettävyyttä vaarantavien tilanteiden varalta. Määräyksen mukaan teleyrityksellä on oltava valmiudet ryhtyä toimenpiteisiin, joilla tälläistä toimintaa voidaan rajoittaa. (13/2005 M, 6§.)

Teleyritykset ovat velvoitettuja estämään sellaisen yhdysliikenteen välittäminen, jonka lähdeosoite ei ole lähettävän teleyrityksen reittimainostuksessa. Teleyritysten tulee suodattaa omaan verkkoon suuntautuva liikenne, jonka lähdeosoite on osoitettu kyseiselle teleyritykselle. Määräyksen mukaan myös julkiseen internetverkkoon suunnattujen yleislähetysviestin välitys on estettävä. Määräys myös velvoittaa teleyritykset seuraamaan tarjoamiensa yhteyspalvelujen laatua ja palveluvarmuutta. (13/2005 M, 7 - 9§.)

5.7.3 Tietoturvaloukkauksista ilmoittaminen

Viestintäviraston määräys tietoturvaloukkausten sekä vika- ja häiriötilanteiden ilmoittamisvelvollisuudesta yleisessä teletoiminnassa (9 B/2004 M, 2§) velvoittaa teleyrityksen ilmoittamaan Viestintävirastolle havaitusta merkittävästä tietoturvaloukkauksesta. Myös mahdollinen uhka tulee ilmoittaa.

Sähköisen viestinnän tietosuojalain 21 §:n 1 momentin mukaisessa erityistä uhkaa koskevassa ilmoituksessa tilaajalle teleyrityksen tulee selvittää tilaajalle ja käyttäjälle heiltä odotettavat toimenpiteet. Myös heihin vaikuttavat teleyrityksen omat toimenpiteet tulee selvittää tilaajalle. (9 B/2004 M, 2§.)

6 RATKAISUT VOIP:N KÄYTTÄMISEKSI JULKISHALLINNOSSA

6.1 Yleistä

Suomen laki itsessään asettaa valtiolle vaatimukset tietoturvaa ajatellen. On todella hyvä, että tietoturva on otettu huomioon lainsäädännössä. Tämä pakottaa organisaatiot ja yhteisöt miettimään tietoturvan merkitystä, omaa tietoturvaa ja tietoturvaratkaisuja.

Valtiovarainministeriö vastaa valtion IT-toiminnasta. Se myös kehittää valtion tietoturvallisuutta asettamansa VAHTI-johtoryhmän kautta. VAHTIiin kuuluu laaja asiantuntijoiden joukko valtion eri toimialoilta ja organisaatioista. Erillisen, tietoturvallisuuteen keskittyvän asiantuntijaryhmän muodostaminen kertoo, että tietoturvan merkitys valtiolle on suuri. Se kertoo myös, että valtio haluaa pysyä tietoteknisen kehityksen kärjessä ja kehittää sitä jatkuvasti.

VAHTI on toiminut jo vuosia tuottaen valtiohallinnon käyttöön useita eri tietoturvaohjeita, -määräyksiä ja -suosituksia. Materiaali on saatavana julkisesti paperilla ja sähköisesti VAHTIn internet-sivulta. Asiantuntevaa tietoa löytyy siis runsaasti ja ne käsittävät koko tietoturvallisuuden alueen. Ohjeet pyrkivät ottamaan huomioon eri tekniikoiden vaatiman tietoturvallisuuden ja ohjeistamaan siinä, miten järjestelmä tulee suunnitella ja rakentaa tietoturvallisuus huomioon ottaen.

IP-puhelut on myös otettu huomioon VAHTIn ohjeistuksessa. Periaatteessa moni ohje ja suositus kattaa myös VoIP-tekniikan, koska se vaatii samantyyppisiä tietoturvaratkaisuja kuin muutkin internet-pohjaiset palvelut. Tämän myötä julkishallinnossa VoIP-järjestelmän suunnittelussa ja rakentamisessa voidaan käyttää VAHTIn aineistoa. VoIP:ssa käytettävien tietoturvaratkaisujen tulee perustua tähän aineistoon.

6.2 VoIP:n tietoturvaratkaisut

6.2.1 VAHTIn aineisto ratkaisujen pohjana

Valtiohallinnon tietoturvaohjeistuksen mukaan tietoliikenneturvallisuuteen kuuluu verkon korkea käytettävyys. Tämän vuoksi VoIP-järjestelmän rakentamisessa suunnittelu on tärkeässä roolissa. Jos VoIP-järjestelmä on tarkoitus rakentaa jo olemassa olevaa verkkoa käyttäen, nykyisen verkon käyttöaste, toimintavarmuus, eheys ja kestävyys tulee tutkia ja mitata ennen VoIP-järjestelmän rakentamista. VoIP:n aiheuttama liikenteen kasvu tulee mitoittaa oikein. Verkon tulee olla kestävä, ja eikä siitä saa löytyä heikkouksia. Lisäksi liikenteen jatkuva kasvu on tärkeää ottaa huomioon. Jos nykyisessä verkossa havaitaan puutteita käytettävyydessä, puutteet tulee korjata tai VoIP:a varten tulee rakentaa uusi verkko.

VAHTIn mukaan julkishallinnon käyttöön tuleva VoIP-järjestelmä tulee luokitella keskeiseksi ja kriittiseksi tietojärjestelmäksi. VAHTI määrittelee VoIP-järjestelmän osat yhtä tärkeäksi kuin muutkin osat organisaation verkossa. Suojaamattomana se on altis hyökkäyksille ja riski tietoturvallisuudelle. VoIP on kriittinen erityisesti siinä tapauksessa, jos VoIP on organisaation ainoa sisäinen puhelinjärjestelmä ja jos IP-puhelut kulkevat organisaatioiden välillä internetin välityksellä. Internet on kanava, jota käytetään nykyään yhä enemmän organisaatioiden väliseen tiedonsiirtoon. Internetin käytön johdosta tiedonsiirto tulee salata. Myös todentamista tulee käyttää luotettavuuden takaamiseksi. Turvallisuutta ajatellen merkittäviä ratkaisuja ovat yksityisten IP-osoitteiden käyttö, VLAN:ien käyttö, VLAN:ien pääsynhallinta, VoIP-palvelimien turvaaminen sekä VoIP- ja dataverkon välisen liikenteen suodattaminen. Lisäksi tarvitaan liikenteen suojausta ja salausta.

6.2.2 Fyysisen ympäristön turvaratkaisut

VoIP-palvelimien on hyvä perustua tunnettuihin ja yleisiin ratkaisuihin. Ne ovat vähintään yhtä tärkeitä kuin muutkin palvelimet, kuten sovellus- tai kirjautumis-

palvelimet. Sen myötä VoIP-palvelimet vaativat samantasoisia tietoturvaratkaisuja.

Palvelimet tulee sijoittaa paikkaan, johon on rajattu ja valvottu sisäänpääsy. Palvelinhuoneen ilmastoinnin riittävyydestä tulee pitää huolta. Palvelinten virransyöttö on tärkeää varmentaa UPS-laitteella. Palvelimien käyttöjärjestelmien päivitykset tulee tehdä säännöllisesti. Toimivuuden takaamiseksi VoIP-palvelinten tulisi olla dedikoituja VoIP-palvelimia, eli ne pyörittävät vain VoIP:n tarvitsemia sovelluksia. Yksi ratkaisu on yksittäiset VoIP-palvelimet, mutta vaihtoehtoinen ratkaisu voi olla palvelimien virtualisointi, jolloin säästöä kertyy rautakustannuksissa. Lisähintaa tulee kyllä virtualisointi-ohjelmistosta, mutta kustannuslaskelmat osoittavat sen, maksaako palvelimien virtualisointiratkaisu itsensä takaisin jossain vaiheessa. Palvelimet tulee sijoittaa palomuurin taakse ja niissä tulee olla ajanmukaiset virustentorjuntaratkaisut.

6.2.3 VoIP-verkon turvaratkaisut

Yksityisten IP-osoitteiden käyttö VoIP-verkossa antaa lisäturvaa. Yksityisosoitteiden käyttö (10.x.x.x, 172.16.x.x ja 192.168.x.x) parantaa entisestään tietoturvaa, koska niitä ei saa reitittää julkisessa internetissä. Osoitteiden erottelu helpottaa myös palomuurien, reitittimien ja kytkimien pääsylistojen hallintaa. VoIP-laitteet ja VoIP:n eri komponentit on hyvä sijoittaa omaan aliverkkoonsa.

Yleisen tietoturvallisuuden ja valtiohallinnon asettamien tietoturvallisuusohjeiden myötä VoIP-verkko tulee eristää organisaation muusta tietoliikenneverkosta. Tämä tapahtuu parhaiten VLAN-ratkaisulla, joka on myös VAHTIn suositus. Fyysisten kaapeleiden vetäminen pelkästään VoIP:aa varten olisi paras ratkaisu, mutta sen ratkaisun myötä kustannukset nousevat liian suureksi. VLAN on selvästi kustannustehokkaampi ratkaisu, ja VLAN:ssa tietoturva on kuitenkin erittäin hyvä. VoIP tulee siis sijoittaa organisaatiossa omaan VLAN:iin, johon kytketään VoIP:n tarvitsemat palvelimet ja käyttäjäagentit eli IP-puhelimet. VLAN:t helpottavat

VoIP-liikenteen hallintaa ja suodattamisesta ja VLAN:t tuovat muutenkin lisäturvaa. Jos suodatusta halutaan tehostaa ja organisaatiossa vaaditaan korkean tason tietoturvaa, VoIP-järjestelmä tulee jakaa useisiin VLAN:eihin. Palvelimet, yhdyskäytävät, VoIP-puhelimet, hallintatyöasemat ja muut VoIP-järjestelmän osat voidaan sijoittaa jokainen omaan VLAN:iin. Tämä järjestely tehostaa suodatusta edelleen.

VLAN:ien pääsynhallinta ehkäisee tunkeilua. Kaikki käyttämättömät portit tulisi liittää käyttämättömään VLAN:iin. Myös IP-puhelimien käyttämättömät portit tulisi ottaa pois käytöstä. Pääsynhallinnan apuna on kytkimien Port Security -ominaisuus, joka käyttää MAC-suodatusta. Toinen vaihtoehto on VMPS-menetelmä. VMPS:n avulla käyttäjä voidaan liittää oikeaan VLAN:iin. VoIP- ja data-VLAN:n välinen liikenne voidaan tarvittaessa estää kokonaan tai liikenne tulee ainakin suodattaa huolellisesti.

Jos käytössä on NAT, se tulee ottaa huomioon VoIP:n suunnittelussa. NAT:n käyttö aiheuttaa ongelmia VoIP-liikenteelle, erityisesti SIP-protokollan kanssa. Myös palomuurit ovat merkittävässä asemassa VoIP-verkossa. VoIP-verkko tulee sijoittaa palomuurin taakse, erityisesti jos VoIP-verkosta on yhteys julkiseen internetiin. Palomuurien tulee olla sellaisia, jotka ymmärtävät VoIP:n SIP-protokollaa. Paras palomuuriratkaisu on tilallinen palomuuri. Palomuurin ja NAT:n avuksi voidaan ottaa ALG- ja FCP -välityspalvelimet. Ne toimivat yhteistyössä palomuurin kanssa antaen SIP-liikenteen kulkea palomuurin läpi. NAT:n aiheuttamat ongelmat voidaan kiertää myös STUN-palvelimella.

6.2.4 Tunnistamis- ja autentikointiratkaisut

SIP-protokolla on VoIP:n käyttämä merkinantoprotokolla, jonka varaan uudet VoIP-järjestelmät kannattaa rakentaa. SIP-protokollassa itsessään ei ole tietoturvamekanismeja, vaan sen SIP-sanomien todentamiseen ja suojaamiseen käytetään HTTP- ja SMTP-protokollista tuttuja tietoturvaratkaisuja. Kun VoIP-liikenne kulkee julkisen internetin yli, VoIP-liikenne tulee turvata huolellisesti, erityisesti kun

kyse on luottamuksellisesta tiedosta. VAHTIn ohjeiden mukaan VoIP:n kanssa tulee käyttää vahvaa salausta. Ratkaisujen tulee toteuttaa myös tiedon eheys ja luotettavuus VAHTIn ohjeiden mukaisesti.

Jos toteutukset tukevat SHA-1- ja 3DES-salausta, SIP-sanomien turvaamiseksi voidaan käyttää S/MIME-salausprotokollaa. S/MIME:ssä käyttäjien tunnistus tapahtuu X.509-varmenteilla. SIPS URI -ratkaisu taas vaatii PKI:n käyttöä. Se on paras ratkaisu, jos verkkoisäntien välillä ei ole luottamussuhdetta. PKI on myös VAHTIn suosittelema tunnustamisratkaisu, joten SIPS URI on näistä suositellumpi vaihtoehto. IPSec:lla voidaan myös salata tietoa, varmistaa tiedon eheys ja todentaa käyttäjä. IPSec:ssa autentikointi voidaan hoitaa PKI-ratkaisulla. IPSec voidaan toteuttaa myös VPN:llä. SIP:n lisäksi RTP-tietovirta voidaan suojata IPSec:lla. IPSec:n käyttö tosin kasvattaa pakettikokoa. Kevyempi ratkaisu olisi SRTP-suojaus, mutta se käyttää PSK-autentikointia, joten se ei ole VAHTIn suositusten mukainen ratkaisu.

Edellä mainittujen lisäksi käyttäjän todennuksessa voidaan käyttää SIP Identity -menetelmää. Siinä soittaja tunnistautuu oman yrityksen palvelimelle. SIP-palvelin allekirjoittaa SIP-sanoman yksityisellä avaimella ja lisää siihen osoitteen, josta vastapuoli voi hakea varmenteen. Vastapuoli hakee varmenteen tästä osoitteesta ja todentaa allekirjoituksen. Näin yritys varmentaa vastapuolelle soittajan olevan se, joka hän väittää olevansa.

Näitä suosituksia käyttäen valtion organisaatiot ja voivat rakentaa VoIP-järjestelmästään tietoturvallisen. Rakentaminen vaatii kuitenkin huolellista suunnittelua ja VoIP-tekniikan ymmärtämistä. VoIP:n kanssa tulee käyttää VAHTIn suosittelemia PKI-ratkaisuja, jotka ovat jo laajalti käytössä valtion eri virastoissa.

7 YHTEENVETO JA JOHTOPÄÄTÖKSET

7.1 VoIP:n soveltuvuus julkishallinnon käyttöön

VoIP:sta on tulossa suosittu puhelinjärjestelmä yrityksille ja organisaatioille. VoIP:n myötä puheluista tulee ilmaisia, koska VoIP voi käyttää hyväkseen yrityksen jo olemassa olevaa tietoliikenneverkkoa eikä sisäverkossa tapahtuvaa liikennettä laskuteta. VoIP:n yleistymisen myötä VoIP tietoturva nousee tärkeäksi haasteeksi.

Valtio on tietoturvallisuusohjeistuksessaan mielestäni ottanut huomioon myös VoIP:n ja sen vähäisen tietoturvan, mitä se pystyy itsessään tarjoamaan. VAHTIn esittämä IP-puheluita koskeva ohjeistus antaa hyvän pohjan VoIP:n saamiseksi tietoturvalliseksi. Lisäksi kun huomioon otetaan muu VAHTIn tietoliikennettä, internet-tietoturvallisuutta, lähiverkkoja ym. koskeva ohjeistus, niin olemassa olevia tietoturvaratkaisuja käyttäen VoIP voidaan rakentaa turvalliseksi puhelinjärjestelmäksi.

VoIP-järjestelmän rakentamisessa tärkeintä on hyvä suunnittelu. VoIP-järjestelmä on tärkeää pitää kriittisenä järjestelmänä. Tietoturvataso tulee mitoittaa kriittisyyden mukaan. VoIP:n turvaamiseksi löytyy hyviä ratkaisuja, kuten VLAN:n käyttöönotto ja erilaiset salaustekniikat. Turvaamista helpottaa se, että VoIP:n ja SIP-protokollan kanssa voidaan käyttää jo olemassa olevia tietoturvaratkaisuja. Nämä suositukset huomioon ottaen valtion organisaatiot ja virastot voivat rakentaa VoIP-järjestelmästään tietoturvallisen. Rakentaminen vaatii kuitenkin huolellista suunnittelua ja VoIP-tekniikan ymmärtämistä. VAHTIn ohjeet toimivat hyvänä ohjenuorana VoIP-järjestelmän saattamiseksi tietoturvalliseksi.

7.2 Työn onnistuminen

Opinnäytetyön tavoitteena oli selvittää VoIP:aa tekniikkana, VoIP:n tietoturvaa ja sitä, miten VoIP sopii julkishallinnon käyttöön valtion tietoturvallisuuden

näkökulmasta. Samoin tavoitteena oli tutkia käyttäjän tunnistautumista VoIP:ssa. Työ oli luonteeltaan teoriapainotteinen tutkimustyö.

Haastavinta oli suomenkielisten, VoIP:n tietoturvaa käsittelevien lähteiden saatavuus. VoIP:sta löytyy jo suomenkielistä materiaalia, mutta VoIP:n tietoturva käsitellään yleensä hyvin pintapuolisesti niissä. Tämän myötä lähteet piti pitkälti etsiä englanninkielisestä materiaalista. Onneksi internet tarjoaa nykyään helpon tavan löytää tietoa lähes aiheesta kuin aiheesta. Haastavaa sen sijaan on löytää tietoa, johon voi luottaa ja jota voidaan pitää luotettavana. USA:n puolustusministeriön teettämää VoIP-tutkimusta voidaan pitää luotettavana lähteenä, samoin IETF:n RFC-dokumenttia. VoIP:n tietoturva-osio pohjautuukin vahvasti näihin kahteen lähteeseen. Samoin VAHTIn asiantuntevat dokumentit ovat helposti saatavissa internetistä.

Työ onnistui hyvin. VoIP:iin kohdistuvista uhkista ja ongelmista löytyi ajanmukaista tietoa. Tietoa löytyi myös teoriapohjaisista ratkaisuista näihin uhkiin ja ongelmiin. Käyttäjän todennus VoIP:ssa oli työn ainoa osa, joka jäi vielä vajavaiseksi. SIP Identity -menetelmästä ei tuntunut löytyvän selkeää käytännön kokemuksiin perustuvaa laajamittaista materiaalia. Englanninkielisiä dokumentteja löytyi kyllä, mutta niitä oli haastavaa lukea niin, että ne myös sisäisti ymmärrettävästi. Ilmeisesti SIP Identity -menetelmä on vielä kovin uusi menetelmä ja se ei ole vielä kovin laajalti käytössä, eikä siitä ole paljon käytännön kokemuksia.

SIP Identity perustuu ilmeisesti kuitenkin siihen, että käyttäjän puhelin tunnistautuu palvelimelle, ei siis varsinaisesti itse käyttäjä. Entä jos puhelinta käyttävä henkilö ei ole se, kuka hän väittää olevansa? Monien VoIP-puhelimien käyttö on salasanan takana, mutta entä jos päätelaitteessa ei ole käytössä edes salasanaa? Tämä voi olla ongelma erityisesti, kun kyse on luottamuksellisista puhelinkeskusteluista ja puhelun osapuolilta vaaditaan ehdotonta luottamusta toisiinsa. Ratkaisu olisi, että käyttäjän tulisi tunnistautua VoIP-puhelimelle tai puhelimen kautta palvelimelle. Tähän voidaan käyttää salasanaa, joka on yksinkertaisin ratkaisu. Vielä parempi ratkaisu olisi, jos VoIP-puhelimessa olisi kortinlukija, jonka kautta organisaation käyttäjä voi tunnistautua toimikortti+salasana-yhdistelmällä.

Kortinlukijan sisältävät VoIP-puhelimet ovat kuitenkin vasta tulossa markkinoille. Käyttäjän todennus jää tämän työn myötä asiaksi, joka kaipaa syvempää analyysia sekä perehtymistä. Siitä saisikin kokonaan uuden opinnäytetyön aiheen.

7.3 Tulevaisuus

VoIP on nousemassa merkittäväksi tekijäksi puhelinliikenteen välittäjänä. Sen yleistymistä Suomessa on kuitenkin ilmeisesti haitannut VoIP-järjestelmien keskeneräisyys ja monimutkaisuus. Ongelmia on ollut mm. äänenlaadun kanssa.

VoIP-järjestelmän kokoaminen vaatii paljon tietämystä. Erityisesti tämän suhteellisen uuden tekniikan osan tietoturva on vaativa osa-alue. Valitettavasti VoIP:n käyttämät protokollat eivät itsessään tarjoa tietoturvaa, mutta onneksi VoIP:n kanssa voi käyttää olemassa olevia tietoturvaratkaisuja. On silti tärkeää muistaa, että minkä tahansa verkon turvaaminen on jatkuva prosessi. Tietoisuus haavoittuvuuksista ja uusimmista ratkaisuista on merkittävässä roolissa. VoIP:n kanssa työskentely vaatii jatkuvaa tietoisuutta tietoturvasta sekä uusimmista ratkaisuista ja suojausmenetelmistä.

SIP-protokollaan tullaan todennäköisesti lähitulevaisuudessa sisällyttämään tietoturvaa. Tämä edesauttaa yhdenmukaisten VoIP-järjestelmien kehittämisessä taaten samalla VoIP-järjestelmien tietoturvallisuuden. IP-tekniikan kehitys ja koeteltu IP-tekniikka auttavat varmasti VoIP-tekniikan läpilyömisessä myös Suomessa lähivuosina. VoIP tarvitsee tähän kuitenkin positiivista nostetta. VoIP:n julkiset uhkat, kuten roskapuhelut eli SPIT yms. eivät ainakaan auta asiaa. VoIP:n täytyy luoda itsestään luotettava, häiriöitä kestävän tekniikan kuva. IP-puhelut on mahdollista toteuttaa turvallisesti käyttäen mm. tässä työssä esille tuotuja turvamenetelmiä. Toivottavasti näiden turvamenetelmien esille tuonti tässä työssä auttaa osaltaan oikeanlaisen VoIP:n tietoturvakuvan rakentamista. VoIP:sta saadaan turvallinen ja toimiva järjestelmä, kun se suunnitellaan ja toteutetaan huolellisesti.

LÄHTEET

Kirjalliset lähteet

Davidson, J. & Peters, J. 2002.Voice over IP. Helsinki: Edita Prima Oy.

Haglund, H. & Wirzenius, A. 2005. Viestintäpalvelujen yleistymisen esteet. Selvitysraportti. Liikenne- ja viestintäministeriön julkaisuja 17/2005. Helsinki. Liikenne- ja viestintäministeriö.

Hämäläinen, P. 2007. IP-puheen tietoturva puhuttaa. Tietokone 1/2007, 49–50.

Karila, A. 2005. Internet-puhelut (VoIP). Selvitys. Liikenne- ja viestintäministeriön julkaisuja 16/2005. Helsinki. Liikenne- ja viestintäministeriö.

Kerttula, E. 1998. Tietoverkkojen tietoturva. Helsinki: Oy Edita Ab.

Volotinen, V. 1999. Tietoliikenne: televerkot ja päätelaitteet. Porvoo: WSOY.

Elektroniset lähteet

3CX. 2007a. Mitä Enum tarkoittaa? [verkkojulkaisu]. 3CX [viitattu 2.2.2007]. Saatavissa: http://www.3cx.fi/voip-sip/enum.php

3CX. 2007b. Mikä on STUN-palvelin? [verkkojulkaisu]. 3CX [viitattu 28.2.2007]. Saatavissa: http://www.3cx.fi/voip-sip/stun-server.php

Defence Information Systems Agency. 2006. Internet Protocol Telephony & Voice over internet Protocol, Security Tehnical Implementation Guide. Version 2, Release 2 [verkkojulkaisu]. Defence Information Systems Agency, Department of Defence [viitattu 8.2.2007]. Saatavissa http://csrc.nist.gov/pcig/STIGs/VoIP-STIG-V2R2.pdf

Ericsson. 2007. SIP - Session Initiation Protocol [verkkojulkaisu]. Ericsson [viitattu 10.1.2007]. Saatavissa: http://www.ericsson.com/fi/technology/SIP.shtml

Koivisto, M. 1997. Tietoliikennetekniikan perusteet [verkkojulkaisu]. Internetix [viitattu 30.1.2007]. Saatavissa: http://www.internetix.ofw.fi/opinnot/opintojaksot/6tekniikkatalous/tietoliikenne/

Mäkinen, M. & Pöyhönen, T. 2004. Voip-tekniikka [verkkojulkaisu]. Jyväskylän yliopisto [viitattu 20.1.2007]. Saatavissa: http://www.cc.jyu.fi/~tmpoyhon/televerkot/Voip2004.htm

Newport Networks. 2005. SIP, Security and Session Border Controllers [verkkojulkaisu]. Newport Networks [viitattu 16.2.2007]. Saatavissa: http://www.newport-networks.com/cust-docs/38-SIP-Security.pdf

Peltola, J. 2002. Megaco-arkkitehtuurin mukainen toteutusratkaisu IP- ja PSTN-puheluissa [verkkojulkaisu]. Tampereen teknillinen yliopisto [viitattu 2.2.2007]. Saatavissa: http://trc.pori.tut.fi/tots/Diplomityo_JPeltola.pdf

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. & Schooler, E. 2002. SIP: Session Initiation Protocol [verkkojulkaisu]. Network Working Group [viitattu 6.2.2007]. Saatavissa: http://www.ietf.org/rfc/rfc3261.txt

SANS Institute. 2007. SANS TOP-20 Internet Security Attack Targets [verkkojulkaisu]. SANS Institute [viitattu 8.2.2007]. Saatavissa: http://www.sans.org/top20/

Steffen, A., Kaufmann, D. & Stricker, A. 2004. SIP Security [verkkojulkaisu]. Zürcher Hochschule Winterthur [viitattu 1.3.2007]. Saatavissa: http://security.hsr.ch/docs/DFN_SIP.pdf

Suomi.fi. 2007a. Julkishallinnon toiminta [verkkojulkaisu]. Suomi.fi [viitattu 14.2.2007]. Saatavissa: http://www.suomi.fi/suomifi/suomi/tietopaketit/julkishallinnon_toiminta/index.html

Suomi.fi. 2007b. Valtionhallinto [verkkojulkaisu]. Suomi.fi [viitattu 14.2.2007]. Saatavissa: http://www.suomi.fi/suomifi/suomi/tietopaketit/julkishallinnon_toiminta/valtionhallinto/index.html

Suomi.fi. 2007c. Ministeriöt [verkkojulkaisu]. Suomi.fi [viitattu 14.2.2007]. Saatavissa: http://www.suomi.fi/suomifi/suomi/tietopaketit/julkishallinnon_toiminta/ministeriot/index.html

Telecomspace. 2006. SIP Overview, Tutorials/Recources [verkkojulkaisu]. Telecomspace [viitattu 10.1.2007]. Saatavissa: http://www.telecomspace.com/vop.html

Valtiovarainministeriö. 2000. Tietojärjestelmäkehityksen tietoturvallisuussuositus [verkkojulkaisu]. Valtiovarainministeriö [viitattu 7.3.2007]. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/3389/3391_fi.pdf

Valtiovarainministeriö. 2003a. Valtion tietohallinnon internet-tietoturvallisuusohje, VAHTI 1/2003 [verkkojulkaisu]. Valtiovarainministeriö [viitattu 14.3.2007]. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/39680/39681_fi.pdf

Valtiovarainministeriö. 2003b. Valtionhallinnon tietoturvakäsitteistö, VAHTI 4/2003 [verkkojulkaisu]. Valtiovarainministeriö [viitattu 14.3.2007]. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/50903/50902_fi.pdf

Valtiovarainministeriö. 2004. Valtiohallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004 [verkkojulkaisu]. Valtiovarainministeriö [viitattu 6.3.2007]. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/90727_fi.pdf

Valtiovarainministeriö. 2006. Tunnistaminen julkishallinnon verkkopalveluissa, VAHTI 12/2006 [verkkojulkaisu]. Valtiovarainministeriö [viitattu 29.1.2007]. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061204Tunnis/Vahti_12_06.pdf

Valtiovarainministeriö. 2007a. Ministeriö [verkkojulkaisu]. Valtiovarainministeriö [viitattu 14.2.2007]. Saatavissa: http://www.vm.fi/vm/fi/02_ministerio/index.jsp

Valtiovarainministeriö. 2007b. Hallinnon kehittäminen [verkkojulkaisu]. Valtiovarainministeriö [viitattu 14.2.2007]. Saatavissa: http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/index.jsp

Valtiovarainministeriö. 2007c. Tietoturvallisuus [verkkojulkaisu]. Valtiovarainministeriö [viitattu 14.2.2007]. Saatavissa: http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/index.jsp

Viestintävirasto. 2007a. ENUM [verkkojulkaisu]. Viestintävirasto [viitattu 2.2.2007]. Saatavissa: http://www.ficora.fi/index/palvelut/enum.html

Viestintävirasto. 2007b. Sähköisen viestinnän tietoturva ja -suoja [verkkojulkaisu]. Viestintävirasto [viitattu 21.3.2007]. Saatavissa: http://www.ficora.fi/index/saadokset/lait/svt.html

Voip-info.org. 2006. SIP [verkkojulkaisu]. Voip-info.org [viitattu 10.1.2007]. Saatavissa: http://www.voip-info.org/wiki-SIP

Westerberg, O. 2006. SIP, Security & Firewalls [verkkojulkaisu]. Ingate Systems [viitattu 18.01.2007]. Saatavissa http://www.sipforum.org/component/option,com_docman/task,doc_download/gid,74/Itemid,75/

Wikipedia. 2007. Session Initiation Protocol [verkkojulkaisu]. Wikipedia [viitattu 30.1.2007]. Saatavissa: http://en.wikipedia.org/wiki/Session_Initiation_Protocol

Lait, asetukset ja säädökset

Määräys internet-yhteyspalvelujen tietoturvasta ja toimivuudesta (Viestintävirasto 13/2005 M). Annettu Helsingissä 3.11.2005.

Määräys sähköpostipalvelujen tietoturvasta ja toimivuudesta (Viestintävirasto 11/2004 M). Annettu Helsingissä 27.8.2004.

Määräys teleyritysten tietoturvasta. (Viestintävirasto 47 B/2004 M). Annettu Helsingissä 27.8.2004.

Määräys tietoturvaloukkausten sekä vika- ja häiriötilanteiden ilmoittamisvelvollisuudesta yleisessä teletoiminnassa (Viestintävirasto 9B/2004 M). Annettu Helsingissä 27.8.2004.

LIITTEET

LIITE 1. Portit ja palvelut, jotka tulee ottaa huomioon palomuuria säätäessä VoIP-palvelimia ja verkkoja varten (Defence Information Systems Agency 2006, 48)

Palvelu	**Porttinumero**
SCCP	TCP 2002-2002
TFTP	UDP 69
MGCP	UDP 2427
Backhaul (MGCP)	TCP 2428
Tapi/Jtapi	TCP 2748
http	TCP 8080/80
HTTPS/SSL	TCP 443
MS päätepalvelut	TPC 3389
VoIP-liikenne	16384-32767
SNMP	UDP 161
SNMP Trap	UDP 162
DHCP (BOOTP)	TCP & UDP 67 & 68
DNS	UDP 53
NTP	UDP 123
LDAP	TCP 389
H.323 Gatekeeper Discovery	UDP 1718
H.323 RAS	UDP 1719
H.323 H.225	TCP 1720
H.323 H.245	TCP 11000-11999
SIP	TCP tai UDP 5060 tai 5061
RTP & RTCP	UDP 1024-65534
DC Directory	TCP 8404
Echo	Echo
Echo-reply	echo-reply
MS-SQL	TCP 1433
SMB	TCP 445
ICCS	TCP 8002
CTIM (CTI Manager)	TCP 8003
CTI/QBE	TCP 2478
SCCP	TCP 3224
HID Agent	TCP 5000

LIITE 2/1. Valtiohallinnon tietoturvallisuusohjeistuksen pohjana käytettävä lainsäädäntö (Valtiovarainministeriö 2004, 99–101)

Laki yksityisyyden suojasta työelämässä (759/2004)

- Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
- sähköisen viestinnän tietosuojalaki (516/2004)

Valtioneuvoston ohjesääntö (262/2003)

- Valtiovarainministeriön toimialaan kuuluvat valtion tietohallinnon, tietojenkäsittelyn ja tietoturvallisuuden yleiset perusteet, hallinnon sähköinen asiointi ja valtioneuvoston yhteinen tietohallinto (17 §)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Laki sähköisistä allekirjoituksista (14/2003)
- Laki turvallisuusselvityksistä (177/2002)
- Valtioneuvoston päätös huoltovarmuuden tavoitteista (350/2002)

Laki valtion talousarviosta annetun lain muuttamisesta (217/2000)

- velvollisuus hoitaa sisäinen valvonta (24 §)
- Suomen perustuslaki (731/1999)
- yksityiselämän suoja (10 §)
- sananvapaus ja julkisuus (12 §)

Henkilötietolaki (523/1999)

- tietoturvallisuus ja tietojen säilytys (7.luku)
- Laki väestötietolain muuttamisesta (527/1999)

Laki viranomaisen toiminnan julkisuudesta (621/1999)

- julkisuusperiaate (1 §)
- velvoite hyvään tiedonhallintatapaan (3 §)
- tiedonsaanti salassa pidettävästä asiakirjasta (10 §)
- viranomaisen velvollisuudet edistää tiedonsaantia ja hyvää tiedonhallintatapaa (5. luku)
- salassapitovelvoitteet (6. luku)
- salassapidosta poikkeaminen ja sen lakkaaminen (7. luku)

Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)

- selvitykset hyvän tiedonhallintatavan toteuttamiseksi (1 §)
- erityissuojattavan tietoaineiston luokitus (2 §)
- erityissuojattavaa tietoaineistoa koskevat yleiset tietoturvallisuustoimenpiteet (3 §)
- ohjeet, valvonta ja seuranta (4 §)
- selosteet tietojärjestelmistä (8 §)

LIITE 2/2. Valtiohallinnon tietoturvallisuusohjeistuksen pohjana käytettävä lainsäädäntö (Valtiovarainministeriö 2004, 99–101)

Henkilökorttilaki (829/1999)

Arkistolaki (831/1994)

- käytettävyys ja säilyminen, tarpeettoman aineiston hävittäminen (7 §)
- turvaaminen tuhoutumiselta, vahingoittamiselta ja asiattomalta käytöltä (12§)
- Laki huoltovarmuuden turvaamisesta (1390/1992)
- Laki julkisista hankinnoista (1505/1992)
- Asetus valtion hankinnoista (1416/1992)

Asetus valtion talousarviosta (1243/1992) sekä sen muutokset (263/2000 ja 254/2004)

- koneellisin menetelmin pidetty kirjanpito ja sen menetelmäkuvaus (47 §)
- sisäinen valvonta (9. luku)
- taloushallinnon järjestelmien tietoturvallisuusmääräykset taloussäännössä (69b §)

Valmiuslaki (1080/1991)

Laki rikoslain muuttamisesta (769/1990)

- luvaton käyttö (28. luku 7 § - 9 §)
- vahingonteko (35. luku 1 § - 3 §)

Laki rikoslain muuttamisesta (578/1995)

- viestintäsalaisuuden loukkaus (38. luku 3 §)
- tietomurto (38. luku 8 §)
- virkasalaisuuden rikkominen (40. luku 5a §)

Laki rikoslain muuttamisesta (951/1999)

- vaaran aiheuttaminen tietojenkäsittelylle (34. luku 9a §)

Tekijänoikeuslaki (404/1961)

- tekijänoikeus suojaa tietokoneohjelmaa (1 §)

Laki Puolustustaloudellisesta suunnittelukunnasta (238/1960)

LIITE 3/1. Tietojärjestelmän elinkaaren eri vaiheiden tietoturvallisuustarkistuslistat (Valtiovarainministeriö 2000, 44–49)

Esitutkimusvaiheen tietoturvallisuustarkastuslista

- Onko toiminta, johon kehitettävä järjestelmä liittyy, todennäköinen ulkopuolisten/asiaankuulumattomien kiinnostuksen kohde? Onko kehitettävä Voidaanko järjestelmää käyttää väärinkäytösten apuvälineenä?
- Miten varsinainen toiminta aiotaan hoitaa erilaisissa yhteiskunnan kriisitilanteissa, esimerkiksi silloin kun valtakunnalliset tietoliikennepalvelut eivät toimi?
- Tunnetaanko järjestelmän kehittämisessä käytettyjen tekniikoiden ja työvälineiden tietoturvallisuusominaisuudet?
- Tunnetaanko järjestelmän käyttöympäristön (tietoliikenneverkko, palvelimet,…) tietoturvallisuusominaisuudet ja vastaavatko ne vaatimuksia?
- Onko järjestelmällä liittymiä matalamman tietoturvallisuustason järjestelmiin?
- Onko järjestelmällä liittymiä esimerkiksi sidosryhmien järjestelmiin, joiden tietoturvallisuustasosta ei ole tarkkaa tietoa tai tietoturvallisuustaso ei ole järjestelmän vaatimusten mukainen?
- Rakennetaanko järjestelmää valmiista komponenteista, joiden tietoturvallisuusominaisuuksia ei tunneta?
- Onko organisaatiolla käytössään tietoturvallisuustekniikoita, jotka soveltuvat käytettäväksi kehitettävässä järjestelmässä?
- Onko järjestelmän vaatimuksia vastaavan tietoturvallisuustekniikan käytölle lainsäädäntöön tms. syyhyn perustuvia rajoituksia?
- Onko organisaatiolla johdon vahvistamat tietoturvallisuusperiaatteet ja täyttääkö suunniteltu järjestelmä sen vaatimukset?
- Onko selvitetty kaikki järjestelmään liittyvä tietoturvalainsäädäntö?

Määrittelyvaiheen tietoturvallisuustarkastuslista

- Esitutkimusvaiheessa tehdyn tietoturvallisuusluokituksen toteaminen kehittämisen perustaksi
- Järjestelmän ulkoisia liittymiä koskeva riskianalyysi
- Järjestelmän päätoimintojen riskianalyysi
- Yksittäisten tietoturvallisuuskriittisten kohteiden tarkempi riskianalyysi
- Ulkoisten liittymien tietoturvallisuusvaatimusten määrittely
- Järjestelmän päätoimintojen tietoturvallisuusvaatimusten määrittely
- Yksittäisten tietoturvallisuuskriittisten kohteiden tietoturvallisuusvaatimusten määrittely
- Tietoturvallisuusvaatimusten kartoitus järjestelmän käyttäjien näkökulmasta
- Jatkuvuussuunnitelmalle asetettavat vaatimukset tarkennetaan

LIITE 3/2. Tietojärjestelmän elinkaaren eri vaiheiden tietoturvallisuustarkistuslistat (Valtiovarainministeriö 2000, 44–49)

- Turvaamisen testaukselle asetettavat vaatimukset määritellään
- Tietoturvallisuusosaamisen varaaminen projektin käyttöön
- Selvitetään turvaratkaisun valintaa rajoittavat tekijät
- Arvioidaan organisaatiossa sovellettavien peruskontrollien soveltuvuus ja riittävyys
- Määritellään lisäkontrollien tarve
- Kartoitetaan mahdolliset tietoturvallisuusratkaisut
- Arvioidaan, miten vaihtoehtoiset ratkaisut täyttävät asetut vaatimukset
- Arvioidaan lisäturvaamisen kustannukset ja vertaillaan niitä riskien taloudellisiin vaikutuksiin yleisesti
- Turvaamisen kustannusvaikutusten tarkempi arviointi
- Arvioidaan jäännösriski yleisesti
- Arvioidaan tietoturvallisuuskriittisten kohtien jäännösriski
- Varmistetaan sovittujen tietoturvallisuusmenettelyjen noudattaminen projektityössä
- Laaditaan turvaamisen alustava testaussuunnitelma
- Laaditaan jatkuvuussuunnitelman alustava versio
- Arvioidaan käytettäviin ohjelmistokehitysvälineisiin liittyvät riippuvuusriskit
- Arvioidaan ohjelmistokehitysvälineiden tietoturvallisuusominaisuudet, määrittely pitäisi tehdä yleensä välineistä vielä välittämättä. Tieturvallisuusvaatimusten pohjalta voi kuitenkin tulla vaatimuksia organisaation käytössä oleviin välineisiin
- Käyttäjäroolien ja niiden rajausten määrittely huomioiden vaaralliset työyhdistelmät
- Kirjausketju -tarpeiden määrittely. Alustava suunnitelma tarpeiden toteuttamistavasta
- Eheyssääntöjen määrittely
- Alustava suunnitelma tietojen eheyden säilyttämisen menettelytavoista
- Kehityksen aikaisten turvaratkaisujen määrittely.

Suunnitteluvaiheen tietoturvallisuustarkastuslista

- Kuvataan peruskontrollien soveltamistapa järjestelmän toiminnoissa
- Kuvataan järjestelmäliittymien peruskontrollit
- Selvitetään ja kuvataan järjestelmän keskeisiin toimintaprosesseihin tarvittavat lisäkontrollit
- Selvitetään ja kuvataan tarkasti järjestelmän tietoturvallisuuskriittisiin yksittäisiin toimintoihin tarvittavat lisäkontrollit
- Verrataan kontrolleja ja niiden toteutuksen vaikutusta tietoturvallisuusvaatimuksiin
- Suunnitellaan peruskontrollien testausmenettely

LIITE 3/3. Tietojärjestelmän elinkaaren eri vaiheiden tietoturvallisuustarkistuslistat (Valtiovarainministeriö 2000, 44–49)

- Suunnitellaan järjestelmän keskeisiin toimintoihin liittyvien lisäkontrollien testaus
- Suunnitellaan yksittäisten tietoturvallisuuskriittisten kohteiden kontrollien testaus ja määritellään testausvastuut
- Suunnitellaan käyttäjäryhmät ja käyttövaltuudet
- Varmistetaan, että tietoturvallisuustehtävät sisältyvät seuraaviin vaiheisiin
- Varmistetaan sovittujen tietoturvallisuusmenettelyjen noudattaminen projektityössä
- Määritellään mitä kontrollimekanismeja sovelletaan perustietoturvallisuustason järjestelmissä peruskontrolleiksi ja mitkä ovat korkeamman tietoturvallisuustason järjestelmissä sovellettavia lisäkontrolleja (esimerkkejä liitteenä)
- Suunnitellaan kirjausketjun (audit trail) toteutus
- Suunnitellaan eheyskontrollien toteutus
- Suunnitellaan järjestelmän käyttäjien, johdon ja järjestelmän käytön valvojien koulutus myös tietoturvallisuuden osalta
- Suunnitellaan varmuuskopiontimenettelyt ja palautukset
- Tarvittaessa suunnitellaan salausmenettelyt, avainten jakelu ja kirjanpito sekä varmentamismenettelyt
- Suunnitellaan testiaineistot huomioiden tietojen luottamuksellisuus

Toteutusvaiheen tietoturvatarkastuslista

- Tarkistetaan peruskontrollien toteutus pistokokeina
- Tarkistetaan, että järjestelmän keskeisiin toimintoihin liittyvien kontrollien toteutus on määritysten mukainen.
- Tarkistetaan, että järjestelmän yksittäisiin tietoturvallisuuskriittisiin kohteisiin liittyvät kontrollit vastaavat määrityksiä.
- Määritellään, voidaanko testeissä käyttää lainkaan tuotantoaineistoja
- Varmistetaan, että testauksessa poikkeuksellisesti käytettävä tuotantoaineisto ei sekaannu aidon aineiston kanssa.
- Varmistetaan, että em. aineistoon sisältyvät henkilötiedot ja tietoturvallisuuskriittiset osat tiedoista muutetaan tai että ne pysyvät vain tietojen käyttöön valtuutettujen tiedossa.
- Varmistetaan, ettei mahdollinen poikkeuksellinen tuotantotietojen testikäyttö aiheuta väärinkäytösmahdollisuutta.
- Varmistetaan, että testiaineisto ja testaus kattavat kaikki turvallisuuden kannalta merkittävät tapaukset.
- Tarkistetaan ohjelmiston kriittisten osien lähdekoodi tekijästä riippumattomasti.
- Estetään hyväksyttyjen ohjelmamodulien muutokset
- Tehdään toteutuksen ja testauksen riippumaton tarkastus

LIITE 3/4. Tietojärjestelmän elinkaaren eri vaiheiden tietoturvallisuustarkistuslistat (Valtiovarainministeriö 2000, 44–49)

- Toteutetaan ja testataan käytön aikaisen kehitys- ja testausympäristön sekä tuotantoympäristön turvaaminen
- Tarkennetaan tietoturvallisuuskuvaukset, rakenteellisuus ja dokumentointi
- Varmistetaan sovittujen tietoturvallisuusmenettelyjen noudattaminen projektityössä
- Tarkistetaan käyttäjien toimintoihin liittyvien peruskontrollien toteutus
- Tarkistetaan käyttäjien toimintoihin liittyvien kontrollien kokonaisuus sekä keskeisiin prosesseihin liittyvät kontrollit
- Varmistetaan, että yksittäisiin tietoturvallisuuskriittisiin käyttäjien toimintoihin liittyvien kontrollien toteutus vastaa asetettuja vaatimuksia.
- Varmistetaan, että käyttäjien koulutussuunnitelmaan sisältyy peruskontrollien käyttökoulutus.
- Varmistetaan, että käyttäjien koulutussuunnitelmaan sisältyy lisäkontrollien käyttökoulutus.
- Tarkistetaan tarvittaessa koulutussuunnitelma yksityiskohtaisesti kontrolleihin liittyvän koulutuksen osalta.
- Varmistetaan sovittujen tietoturvallisuusmenettelyjen noudattaminen projektityössä
- Luetteloidaan toiminnalliset puutteet ja virheet, jotka on korjattava ennen järjestelmän siirtoa tuotantoon. Laaditaan korjausten toteutus- ja testaussuunnitelma

Käyttöönottovaiheen tietoturvallisuustarkastuslista

- Rinnakkaisajon tulosten vertaaminen kontrollien osalta
- Tarkistetaan lisäkontrollien testaussuunnitelma
- Varmistetaan, että testaussuunnitelma kattaa kaikki järjestelmän määrityksiin sisältyvät kontrollit
- Tarkistetaan peruskontrollien testitulokset
- Tarkistetaan lisäkontrollien testitulokset
- Valvotaan kriittisiin toimintoihin liittyvien kontrollien testausta
- Tuotantoaineiston mahdollisen poikkeuksellisen testauskäytön osalta noudatetaan toteutusvaiheessa kuvattuja menettelytapoja
- Luetteloidaan toiminnalliset puutteet ja virheet, jotka voidaan korjata tuotantoon siirron jälkeen ylläpitotyönä. Tehdään ylläpitosuunnitelma
- Varmistetaan sovittujen tietoturvallisuusmenettelyjen noudattaminen projektityössä
- Varmistetaan, että järjestelmän perustietojen latauksessa noudatetaan peruskontrolleja
- Valvotaan perustietojen latauksen kontrollien toimivuutta

LIITE 3/5. Tietojärjestelmän elinkaaren eri vaiheiden tietoturvallisuustarkistuslistat (Valtiovarainministeriö 2000, 44–49)

- Tarkistetaan toistuvasti kaikki turvallisuuden kannalta merkittävät kontrollit perustietojen latauksessa
- Varmistetaan tuotanto-organisaatiolta, että uuden ohjelmiston asennuksessa noudatetaan peruskontrolleja
- Tarkistetaan pistokokeina ohjelmiston asennuksen kontrollit
- Tarkistetaan, että ohjelmistoasennuksen kontrollit ovat asetettujen vaatimusten mukaiset
- Varmistetaan, että käyttäjien koulutus kontrolleihin liittyen on tehty hyväksytyn koulutussuunnitelman mukaisesti
- Varmistetaan, että kaikki käyttäjät ovat saaneet kontrolleja koskevan koulutuksen
- Varmistetaan käyttäjäorganisaatiolta, että käyttäjien toimintoihin liittyvät kontrollit vastaavat vaatimuksia
- Tarkistetaan pistokokeina käyttäjien toimintoihin liittyvät tuotantoympäristön kontrollit
- Tarkistetaan, että käyttäjien toimintoihin liittyvät kontrollit tuotantoympäristössä ovat vaatimusten mukaiset
- Varmistetaan järjestelmän ylläpidosta vastaavilta, että kontrollien ylläpitovastuu sisältyy määriteltyihin ylläpitokäytäntöihin
- Tarkistetaan pistokokeina ylläpitäjien järjestelmädokumentaatio
- Tarkistetaan, että ylläpitäjien dokumentaatioon sisältyy kattava kontrollien kuvaus ja että ylläpitomenetelmät varmistavat vaatimusten mukaisen tietoturvallisuustason säilymisen
- Varmistutaan sovittujen tietoturvallisuusmenettelyjen noudattamisesta
- Varmistetaan, että hyväksymistestaus kattaa muun muassa seuraavat kokonaisuudet:
    - Pääsynvalvontamenettelyjen toimivuus
    - Järjestelmän toiminta normaalissa kuormitustilanteessa ja huippukuormituksella
    - Järjestelmän ”kaatuminen” ja vakavat laitehäiriöt
    - Vakavasta virheestä toipuminen (sekä tekniset asiat että käyttäjien toimenpiteet)
    - Järjestelmän perustietojen lataus
    - Tuotannon aikaisen kehitys- ja testausympäristön hallinta
    - Käyttäjien toimintoihin liittyvät kontrollit
    - Järjestelmän teknisessä toteutuksessa
    - Käyttäjien toiminnoissa
    - Käyttöhenkilöstön toimintoihin liittyvät kontrollit
- Varmistetaan onko tietoturvallisuussuunnitelma tehty?
- Varmistetaan onko tietoturvallisuusohjeisto tehty?
- Varmistetaan onko tärkeysluokka määritelty?
- Varmistetaan onko jatkuvuussuunnitelma tehty?

LIITE 3/6. Tietojärjestelmän elinkaaren eri vaiheiden tietoturvallisuustarkistuslistat (Valtiovarainministeriö 2000, 44–49)

- Varmistetaan sisältyykö jatkuvuussuunnitelmaan toipumissuunnitelma?
- tiedotussuunnitelma?
- yhteyshenkilöt?
- Varmistetaan onko varajärjestelmää, onko varajärjestelmä testattu?
- Varmistetaan onko käyttöoikeusmenettelyt kuvattu ja ohjeistettu?
- Varmistetaan onko järjestelmäseloste tehty ohjeiden mukaisesti?
- Tarkistetaan henkilötietojen suojaaminen

Ylläpitovaiheen tietoturvatarkastuslista

- Lainsäädännön velvoitteiden läpikäynti ja huomiointi
- Varmistetaan, että muutos on perusteltu ja päätös sen tekemisestä on asianmukaisesti hyväksytty.
- Varmistetaan, että muutoksessa otetaan huomioon järjestelmän alkuperäiset suunnittelukriteerit turvallisuuden kannalta. Poikkeamat perusteltava.
- Selvitetään muutoksen vaikutukset muihin kuin muutettavaan kohteeseen epätoivottujen sivuvaikutusten välttämiseksi.
- Selvitetään järjestelmämuutoksen aiheuttamat turvaamisen muutostarpeet yleisellä tasolla
- Selvitetään muutoksen vaikutus järjestelmän keskeisten osien turvaamiseen
- Selvitetään muutoksen vaikutus järjestelmän yksittäisten kriittisten osien turvaamiseen
- Selvitetään tietokannan rakenteen muutosten tietoturvallisuusvaikutukset
- Selvitetään muutoksen vaikutus käyttäjille näkyviin turvaamisiin ja tehdään muutokset käyttöohjeisiin
- Selvitetään vaikutukset tietoturvallisuuden huomioimisesta kehitysympäristön versioinnissa, muutosten dokumentoinnissa sekä koulutusympäristössä
- Laaditaan turvaamisen toteutus- ja testaussuunnitelma resurssivarauksineen
- Varmistetaan, että muutostoimenpiteen hallinnassa noudatetaan tietoturvallisuusluokituksen mukaisia menettelytapoja (soveltaen ensikehitysprojektin toimintamalleja muutoksen laajuutta vastaavasti)
- Varmistetaan, että muutos on testattu kattavasti erillisessä turvallisessa testiympäristössä ennen sen siirtoa tuotantoon
- Tehdään tarvittaessa muutokset jatkuvuussuunnitelmaan
- Testataan jatkuvuussuunnitelman muutokset.

LIITE 3/7. Tietojärjestelmän elinkaaren eri vaiheiden tietoturvallisuustarkistuslistat (Valtiovarainministeriö 2000, 44–49)

Käyttövaiheen tietoturvallisuustarkastuslista

Järjestelmän käyttöön liittyvät toiminnot

Hoidetaan osana järjestelmän käyttötoimintaa turvallisuuteen liittyvät tehtävät, joihin sisältyvät muun muassa

1) Varmistukset ja arkistointi
2) Käyttövaltuuksien hallinta
3) Laitteiden poistot ja vaihdot.

Käsitellään osana jatkuvaa päivittäistä toimintaa järjestelmän toimintaan liittyvät tietoturvallisuushälytykset ja -poikkeamat.

Toipumissuunnitelmien testit

Varmistetaan, että järjestelmän toipumissuunnitelma testataan sovituin määrävälein sovitussa laajuudessa.

Järjestelmän tarkastus määrävälein

- Tehdään tietoturvallisuustarkastus tarvittaessa.
- Tarkistetaan tietoturvallisuuslokit ja analysoidaan havaitut poikkeamat ja ”läheltä piti” -tilanteet.
- Tarkistetaan peruskontrollien toimivuus.
- Selvitetään kontrollien merkittävimmät heikkoudet.
- Selvitetään syyt kontrollien pettämiselle.
- Määritellään tarkastuksen perusteella, ovatko käytettävyys-, eheys- ja luottamuksellisuusvaatimukset muuttuneet alkuperäisistä.

Havaintojen / analyysin perusteella tehtävät toiminnot

- Tehdään tarvittaessa suositus järjestelmän tärkeysluokan tai tietoaineiston luokituksen ja kontrollien muutoksista (esitutkimus-kohta 6.1).
- Tehdään suositus kontrollien muutoksista.
- Tehdään perusteltu ehdotus kontrollien muutoksista. Sisällytetään ehdotukseen arvio kontrollien muutosten toiminnallisista ja kustannusvaikutuksista.

LIITE 3/8. Tietojärjestelmän elinkaaren eri vaiheiden tietoturvallisuustarkistuslistat (Valtiovarainministeriö 2000, 44–49)

Versionvaihtovaiheen tietoturvallisuustarkastuslista

Tietojen siirto vanhasta järjestelmästä uuteen

1) Varmistetaan, että tiedon siirron suunnitelma sisältyy versionvaihdon projektisuunnitelmaan
2) Varmistetaan, että siirtosuunnitelmassa on kuvattu toimenpiteet, joilla varmistetaan tiedon siirron täydellisyys sekä siirrettävien tietojen eheys
3) Varmistetaan, että siirtotoimenpiteet testataan testiaineistolla ennen tuotantoaineistojen siirtoa. Tarkistetaan testitulokset.
4) Varmistetaan, että siirrossa tehtävät välitallennukset eivät vaaranna tiedon luottamuksellisuutta
5) Tarkistetaan, että tiedon siirto uuteen järjestelmään on tehty hyväksytyn suunnitelman mukaisesti.

Tehdään jatkuvuussuunnitelmiin tarvittavat muutokset. Testataan suunnitelman toimivuus mahdollisuuksien mukaan.

Varmistetaan sovittujen tietoturvallisuusmenettelyjen noudattaminen projektityössä.

Käytöstä poistovaiheen tietoturvallisuustarkastuslista

- Tehdään turvaamisen ylläpitosuunnitelma niille järjestelmille, joiden toimintaan poistettavalla järjestelmällä on vaikutusta
- Selvitetään poistettavan järjestelmän aineistoja koskevat arkistointivelvoitteet arkistonmuodostussuunnitelmasta
- Laaditaan hävittämissuunnitelma niille tietoaineistoille, joita ei ole tarpeen arkistoida
- Suunnitellaan poistettavan järjestelmän laitteistojen uudelleenkäyttökohteet tai hävittämismenettelyt
- Tehdään muutokset jatkuvuussuunnitelmiin.
- Toteutetaan poisto sekä mahdolliset arkistoinnit ja laitteistojen sijoittaminen uuteen käyttökohteeseen suunnitelmien mukaisesti pitäen kirjaa tehdyistä toimenpiteistä
- Varmistetaan sovittujen tietoturvallisuusmenettelyjen noudattaminen poistamistoimenpiteissä.

LIITE 4/1. Tietoliikenneturvallisuuden vaatimukset ja niiden pohjana oleva VAHTI-aineisto (Valtiovarainministeriö 2006)

Fyysisen tietoliikenneturvallisuuden keskeiset vaatimukset

- Suojattavat kohteet oltava kuvattu (2/2001)
- Suojausmenetelmien oltava kuvattu (2/2001)
- Aktiivilaitteet ja kaapelointi suojattava ulkopuolisilta (5/2004)
- Verkon kokoonpanon ja asetusten oltava kirjallisessa muodossa (2/2001) (5/2004)
- Verkon rakentamisesta ja ylläpidosta oltava ohjeet (2/2001) (5/2004)
- Eri turvaluokan verkkoja ei yhdistetä (2/2001)
- Verkko jaettava vyöhykkeisiin (2/2001) (5/2004)
- Vyöhykkeet segmentoitava (2/2001)
- Käytettävä teknologiaa, joka rajoittaa tarpeetonta liikennettä (2/2001)
- Kaapelikanavien on oltava suojattuja, vältettävä häiriölähteitä (2/2001)
- Kaapelikanavien on oltava äänieristettyjä (2/2001)
- Kaapelikanavien oltava sinetöitävissä (2/2001)
- Kaapelit nimiöitävä molemmista päistä (2/2001)
- Erityis- ja täyssuojaus vaativat vähintään yhtä täysin erillistä varareittiä (1/2002)
- Käyttämättömät verkkoliitännät poistettava käytöstä (3/2004)
- Kiinteistönvalvontaverkko erillinen muista tietoverkoista (5/2004).

Loogisen tietoliikenneturvallisuuden keskeiset vaatimukset

- Suojattavat kohteet oltava kuvattu (2/2001)
- Suojausmenetelmien oltava kuvattu (2/2001)
- Verkon kokoonpanon ja asetusten oltava kirjallisessa muodossa (2/2001) (5/2004)
- Verkon rakentamisesta ja ylläpidosta oltava ohjeet (2/2001) (5/2004)
- Eri turvaluokan verkkoja ei yhdistetä (2/2001)
- Verkko jaettava vyöhykkeisiin (2/2001) (5/2004)
- Vyöhykkeet segmentoitava (2/2001)
- Käytettävä teknologiaa, joka rajoittaa tarpeetonta liikennettä (2/2001)
- Verkkoon kytkettävät laitteet oltava tunnistettavissa verkosta (2/2001)
- Luottamuksellinen tiedonsiirto salattava (4/2001)
- Tietoliikennejärjestelmän käyttö on valvottua (4/2002)
- Ip-puhelinjärjestelmä erotettava muusta verkosta (1/2003)
- Vahvemman ja heikomman turvavyöhykkeen välinen ftp- ja http-liikenne käytettävä haittamateriaalitorjunnan läpi (3/2004)
- Kriittiset palvelimet, testijärjestelmät, tuotantojärjestelmät ja työasemat erotettava omiksi kokonaisuuksikseen (3/2004)
- Tietoliikenneverkosta oltava tietovirta-analyysi (5/2004).

LIITE 4/2. Tietoliikenneturvallisuuden vaatimukset ja niiden pohjana oleva VAHTI-aineisto (Valtiovarainministeriö 2006)

Pääsynhallinnan vaatimukset

- Jos asiointi ei sitä edellytä, voitava asioida anonyymina (1/2001)
- Julkisen ja salassa pidettävän aineiston järjestelmät erotettava (1/2001) (4/2001)
- Sekä julkisen että salassa pidettävän tiedon järjestelmät suojattava (4/2002)
- Internet-verkkoon ei kytkeydytä ilman palomuuriratkaisua (1/2001)
- Viranomaisten välinen Internetin tms. kautta kulkeva liikenne salattava (1/2001)
- Salassa pidettävä tieto suojataan erillisellä palomuuriratkaisulla (1/2001)
- Etähallinta vaatii vahvaa salausta ja vahvaa tunnistamista (1/2001)
- Kriittisiä järjestelmiä ei hallita etänä (1/2001)
- Vain määritellyt palvelupyynnöt hyväksytään (4/2001)
- Järjestelmiin pääsy on valvottua ja luvaton yritys torjutaan (4/2002)
- Tieto ja järjestelmät vain oikeutettujen saatavilla (4/2002).

Verkkoliikenteen turvaamiseen liittyvät seuraavat estovaatimukset

- luvattomasta lähteestä tulevat yhteydenotot verkon aktiivilaitteeseen muualta kuin lähiverkosta saapuva kyseisen lähiverkon osoitetta lähdeosoitteena käyttävä liikenne (ip address spoofing) estetään
- varattuja osoitteita (RFC 1918) käyttävä liikenne, joka joko saapuu organisaation on verkon ulkopuolelta tai suuntaa sinne
- ICMP-liikenne, jota ei ole listattu RFC 2979:ssä
- luvattomasta osoitteesta saapuva SNMP-liikenne
- organisaation ulkopuolelta saapuva lähdereititystietoa sisältävä liikenne
- lähtevä tai saapuva liikenne, jonka lähde- tai kohdeosoite on 127.0.0.1 tai 0.0.0.0
- liikenne, jonka lähde- tai kohdeosoite on lähiverkon broadcast-osoite.

Päätelaitteen verkkoliitännän suojaamisen vaatimukset

- Hallintayhteydet ja -tavat määriteltävä ja rajattava (2/2003)
- Tarpeeton liikenne on jätettävä käsittelemättä molempiin suuntiin (2/2003)
- Etäkäytössä sallitaan vain määritellyllä tavalla suojatut yhteydet (2/2003)
- Etäkäyttöön käytetään vain määriteltyjä yhteyksiä (2/2003)
- Etäkäyttöliikenteen kuljettava määritellyn palomuuriratkaisun kautta (2/2003)
- Langattoman paikallisverkon laitteita kohdellaan kuin Internetiä (2/2003)
- Oletushallinnointisalasanat ja -tunnukset vaihdettava (2/2003)
- Verkkotunnisteet muutettava (2/2003)

LIITE 4/3. Tietoliikenneturvallisuuden vaatimukset ja niiden pohjana oleva VAHTI-aineisto (Valtiovarainministeriö 2006)

- Langattoman verkon käyttö vaatii käyttäjän tunnistamisen ja todentamisen (2/2003)
- Langaton SNMP-käyttö estettävä (2/2003)
- Langattoman verkon tunnisteiden broadcast on kielletty (2/2003)
- Wakeup on LAN (WOL) estettävä (3/2004).

Verkkoyhteyksien suojaamisen vaatimukset (2/2003)

- Muu kuin suora yhteys organisaatioon vaatii yhteyden suojaamista
- Suojaamisessa käytettävä julkisiin suosituksiin perustuvia ratkaisuja
- Allekirjoittamaton julkinen avain välitettävä off-band
- Etäkäyttöyhteydet on todennettava hyväksytyllä todentamistavalla.

Palvelujen verkkoliitännän suojaamisen vaatimukset (2/2003)

- Etäkäytettävät palvelut luokiteltava
- Eri palvelut eristettävä toisistaan
- Suojausratkaisujen oltava organisaation määrittelemiä
- Pääsynvalvonta palveluihin tapahtuu palvelujärjestelmän eteisverkossa
- VPN-yhteyksiä ei viedä palomuuriratkaisun ohi
- Ulkoisten palvelujen palvelimet erotettava sisäisten palvelujen palvelimista
- Tuki- ja turvajärjestelmien asetukset standardoitava
- Sallittu tietoliikenne on kuvattava ja tietoliikenne rajattava kuvattuun.

Turvaluokitellun tiedon käsittelysäännöt verkossa

- I turvaluokka ei sähköisissä tietojärjestelmissä (1/2001)
- II ja III turvaluokka tarkoituksenmukaisesti salattua (1/2001) (4/2001) (4/2002)
- Pääsynvalvonta (1/2001) (4/2002)
- Käytön valvonta (4/2002)
- Luokiteltua tietoa saa käsitellä selväkielisesti vain organisaation omassa verkossa (4/2002)
- Luokitellun tiedon pääsy sivullisten tietoon pitää estää (4/2002).

Salauksen säännöt (3/2001)

- Symmetrisen salauksen avainpituus väh. 128 bittiä
- Asymmetrisen salauksen avainpituus väh. 1024 bittiä
- Tiivisteen pituus tiivistefunktiossa väh. 128 bittiä [huom: kiinalaiset!]
- Salausavaimet mahdollisimman harvojen hallussa
- Joka käyttökohteessa ja -tilanteessa uusi avain

LIITE 4/4. Tietoliikenneturvallisuuden vaatimukset ja niiden pohjana oleva VAHTI-aineisto (Valtiovarainministeriö 2006)

- Istuntoavaimet erotettava niiden lähettämisessä käytettävistä avaimista
- Istuntoavaimet erotettava tunnistus- ja todennusavaimista
- Avainten pituus suhteutettava avaimen voimassaoloaikaan
- Avainten pituus suhteutettava suojattavan tiedon arkaluontoisuuteen
- Lainsäädännön noudattaminen (3/2002).

Verkkopalveluiden suunnittelu ja toteutus

- JHS 129, palvelun toteutuksen prosessi ja hankinnan ominaisuudet
- JHS 129, ulkoistamisen tarpeiden arviointi ja toteutus
- JHS 129, käytettävyyden kehittämisen menetelmät
- JHS 129, julkiset verkkopalvelut ja lainsäädäntö.